CENTRO ALTI STUDI
PER LA DIFESA

ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

Federica Di Camillo e Ottavia Credi

Fattori d'impatto sull'innovazione tecnologica e sviluppo di capacità Dual-use della Difesa

(Codice AQ-GAB-01)

ISTITUTO DI RICERCA E ANALISI DELLA DIFESA

L'Istituto di Ricerca e Analisi della Difesa (di seguito IRAD), per le esigenze del Ministero della Difesa, è responsabile di svolgere e coordinare attività di ricerca, alta formazione e analisi a carattere strategico sui fenomeni di natura politica, economica, sociale, culturale, militare e sull'effetto dell'introduzione di nuove tecnologie che determinano apprezzabili cambiamenti dello scenario di difesa e sicurezza, contribuendo allo sviluppo della cultura e della conoscenza a favore della collettività e dell'interesse nazionale.

L'IRAD, su indicazioni del Ministro della difesa, svolge attività di ricerca in accordo con la disciplina di Valutazione della Qualità della Ricerca e sulla base della Programma nazionale per la ricerca, sviluppandone le tematiche in coordinamento con la Direzione di Alta Formazione e Ricerca del CASD.

L'Istituto provvede all'attivazione e al supporto di dottorati di ricerca e contribuisce alle attività di Alta Formazione del CASD nelle materie d'interesse relative alle aree: Sviluppo Organizzativo; Strategia globale e sicurezza/Scienze Strategiche; Innovazione, dimensione digitale, tecnologie e cyber security; Giuridica.

L'Istituto opera in coordinamento con altri organismi della Difesa e in consorzio con Università, imprese e industria del settore difesa e sicurezza; inoltre, agisce in sinergia con le realtà pubbliche e private, in Italia e all'estero, che operano nel campo della ricerca scientifica, dell'analisi e dello studio.

L'Istituto, avvalendosi del supporto consultivo del Comitato scientifico, è responsabile della programmazione, consulenza e supervisione scientifica delle attività accademiche, di ricerca e pubblicistiche.

L'IRAD si avvale altresì per le attività d'istituto di personale qualificato "ricercatore della Difesa, oltre a ricercatori a contratto e assistenti di ricerca, dottorandi e ricercatori post-dottorato.

L'IRAD, situato presso Palazzo Salviati a Roma, è posto alle dipendenze del Presidente del CASD ed è retto da un Ufficiale Generale di Brigata o grado equivalente che svolge il ruolo di Direttore.

Il Ministro della Difesa, sentiti il Capo di Stato Maggiore dalla Difesa, d'intesa con il Segretario Generale della Difesa/Direttore Nazionale degli Armamenti, per gli argomenti di rispettivo interesse, emana le direttive in merito alle attività di ricerca strategica, stabilendo le linee guida per l'attività di analisi e di collaborazione con le istituzioni omologhe e definendo i temi di studio da assegnare all'IRAD.

I ricercatori sono lasciati liberi di esprimere il proprio pensiero sugli argomenti trattati: il contenuto degli studi pubblicati riflette quindi esclusivamente il pensiero dei singoli autori e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali i Ricercatori stessi appartengono.

Federica Di Camillo e Ottavia Credi

Fattori d'impatto sull'innovazione tecnologica e sviluppo di capacità Dual-use della Difesa

(Codice AQ-GAB-01)

Le autrici intendono ringraziare Luigi Lo Porto, Tirocinante del Programma Sicurezza dello IAI nel periodo gennaio-aprile 2022, per il prezioso supporto alle attività di ricerca e analisi e il valido contributo alla redazione del testo.

Si ringraziano per la competente disponibilità all'analisi: Dott. Giuseppe G. Daquino, EDA Materials CapTech Chair & ANDES Project Owner; Dott. Giancarlo La Rocca, Ricercatore Junior nei Programmi Difesa e Sicurezza, IAI; Ing. Cristina Leone, Presidente del CTNA; Dott. Alessandro Marrone, Responsabile del Programma Difesa dello IAI & docente di Politica Militare presso ISSMI; Ing. Giorgio Mosca, Sr. VP Strategic Intelligence and Analysis, Leonardo; Prof. Michele Nones, Coordinatore del Cluster CBRN-P3 & Vice Presidente dello IAI; Cons. D'Amb. Roberto Orlando, Capo Divisione beni duali, MAECI; Avv. Marco Padovan, Studio Legale Padovan; Ing. Fulvia Quagliotti, Presidente del Distretto Aerospazio Piemonte; Dott.ssa Luisa Riccardi, Direttore generale del V Reparto del SGD/DNA; CA (Aus) Ing. Francesco Scialla, già Capo Ufficio Ricerca del SGD, Rappresentante del SGD presso la UE & attualmente Membro della Delegazione Italiana al Comitato Cluster 3 di Horizon Europe.

NOTA DI SALVAGUARDIA

Quanto contenuto in questo volume riflette esclusivamente il pensiero dell'autore, e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali l'autore stesso appartiene.

NOTE

Le analisi sono sviluppate utilizzando informazioni disponibili su fonti aperte.

Questo volume è stato curato dall'**Ufficio Studi, Analisi e Innovazione dell'IRAD**.

Direttore
Col. c. (li) s. SM Gualtiero Iacono

Capo dell'Ufficio Studi, Analisi e Innovazione
Col. AArnn Pil. Loris Tabacchi

Progetto grafico
Ass. Amm. Massimo Bilotta – 1° Mar. Massimo Lanfranco – C° 2ª cl. Gianluca Bisanti – Serg. Manuel Santaniello

Revisione e coordinamento
Magg. (AM) Luigi Bruschi - Funz. Amm. Aurora Buttinelli – Ass. Amm. Anna Rita Marra

Autrici
Federica Di Camillo e Ottavia Credi

Stampato dalla Tipografia del **Centro Alti Studi per la Difesa**

Istituto di Ricerca e Analisi della Difesa
Ufficio Studi, Analisi e Innovazione
Palazzo Salviati - Piazza della Rovere, 83 - 00165 – Roma
tel. 06 4691 3205
e-mail: irad.usai.capo@casd.difesa.it

chiusa a aprile 2022 – pubblicato giuno 2022

ISBN 979-12-5515-004-6

Indice

EXECUTIVE SUMMARY (It)

Lo studio si colloca in un periodo di particolare dibattito sul ruolo delle Forze Armate. Nel momento in cui si scrive, il conflitto russo-ucraino è nel pieno del suo svolgimento. Le implicazioni sui modelli di operatività dello strumento militare e sugli investimenti non sono ancora definite, ma saranno profonde e di medio-lungo periodo ai livelli nazionale, UE e NATO.

L'analisi è volta a descrivere fattori che influenzano i processi di innovazione dual-use, sia come Ricerca e Sviluppo (R&S), che come trasferimento di tecnologie e prodotti in applicazioni del mercato inverso. Un obiettivo che intende valorizzare un ricorso equilibrato al dual-use da parte della Difesa, senza compromissione di capacità specifiche militari e anche con linee di investimento separate: military only e dual-use.

Il Capitolo 1 descrive l'inquadramento del dibattito considerando le difficoltà di definizione che caratterizzano il tema dual-use, e sottolineandone i positivi impatti su interoperabilità, innovazione, e finanziamenti.

Il Capitolo 2 descrive i più significativi fattori di influenza che riguardano il settore privato e il settore pubblico.

Per quel che riguarda il settore privato, si tratta di elementi che le aziende considerano nel valutare fattibilità ed opportunità di scelte di innovazione dual-use. Questi riguardano la tipologia di azienda e le possibili strategie di business, come quelle di sviluppo e diversificazione verso mercati (clienti) e tecnologie e prodotti del mercato inverso. La posizione di partenza in termini di core business strategico/tradizionale ha un peso fondamentale. Più l'azienda si allontana dal proprio core business, maggiori sono i costi non solo economico-finanziari, ma di transazione necessari per estendere, adattare o acquisire competenze valide per il mercato inverso. Sia che queste riguardino conoscenza e accesso a strumenti di finanziamento, sia che riguardino compliance verso quadri normativi in senso lato, dall'export agli standard. È soprattutto quindi la posizione di partenza - e cioè se si tratti di azienda tradizionalmente operante nel mercato civile/sicurezza o militare - ad avere una valenza rispetto alla capacità di superare le barriere di accesso al mercato e a combinarsi con le altre caratteristiche dell'azienda. Per tale ragione, i fattori individuati vengono ulteriormente e distintamente analizzati nei differenti passaggi dal civile/sicurezza verso il militare e viceversa. Il Capitolo 2 riporta anche la descrizione dei principali tratti caratterizzanti l'organizzazione R&S come contesto in cui le scelte aziendali sul dual-use si collocano, inclusa l'interazione con la domanda. Gli aspetti considerati vanno dall'open innovation al ruolo dei technology brokering office interni alle aziende. Dai brick tecnologici e i Commercial Off-the-Shelf (COTS), all'incidenza dei diversi livelli di Technology

Readiness Level (TRL). Vengono inoltre forniti esempi concreti di realizzazione di processi di R&S dual-use e trasferimento di tecnologie e prodotti in applicazioni del mercato inverso.

Per quel che riguarda il settore pubblico, si descrivono elementi la cui impostazione è sostanzialmente in capo alle organizzazioni pubbliche, ma che impattano direttamente o indirettamente anche le aziende. I macro-temi analizzati riguardano la domanda, la conoscenza della tecnologia, la governance dei finanziamenti pubblici e le normative.

Da questi macro-temi, nel capitolo 3, sono selezionati alcuni fattori su cui potrebbe positivamente agire il settore pubblico per favorire l'innovazione dual-use.

Quanto alla domanda pubblica, questa è centrale nell'innovazione. Una prima raccomandazione riguarda la necessità di un'analisi comparata dei diversi sistemi di procurement di amministrazioni potenzialmente adatte a sinergie dual-use. Una delle finalità dovrebbe essere valutare se sia possibile – in alcune aree di interesse compatibile o comune tra diversi Ministeri/Enti degli ambiti civile/sicurezza e militare – formulare una domanda basata sulle funzioni, per estendere la ricerca di soluzioni in settori inversi e senza escludere modelli di open innovation. Nelle aree in cui si rilevino funzioni compatibili o comuni dovrebbe essere verificata la possibilità di stabilire meccanismi per definire requisiti tecnici comuni/duali, inclusi adattamenti a requisiti espressi e formalizzati da amministrazioni centrali o locali del settore inverso. L'innovazione dual-use resta direttamente proporzionale alla compatibilità tra standard dei diversi ambiti e alla possibilità di standard ibridi. Il *Piano d'azione sulle sinergie tra l'industria civile, della difesa e dello spazio*, stabilisce che la Commissione europea presenterà entro la fine del 2022 un Piano per promuovere l'uso degli standard ibridi esistenti e lo sviluppo di nuovi. A livello italiano, le azioni su tutti i temi sopra descritti, secondo diversi esperti, sarebbero opportunamente incardinate in un Tavolo Tecnico decisionale presso la Presidenza del Consiglio dei Ministri, con un livello politico e un livello operativo con gruppi di lavoro focalizzati per tematiche (anche per selezionare iniziali settori di interesse dual-use) e gestiti con obiettivi e scadenze.

La conoscenza di tecnologie e di prodotti disponibili o in via di sviluppo e potenziali applicazioni è uno dei fattori più cruciali per l'incontro tra domanda e offerta nell'innovazione dual-use. Il settore pubblico dovrebbe individuare gli strumenti più adatti a tal fine. Tra questi sono di particolare interesse, quelli che possono essere declinati in maniera specifica allo scopo. Quanto alle strutture di technology brokering esterne alle aziende potrebbero essere intese come hub per il trasferimento tecnologico, con un forte grado di neutralità, quindi istituzionale, supportate da investimenti pubblici e strettamente inserite nel contesto europeo. Quanto ai cluster tecnologici/industriali, si deve valutare l'opportunità di creare un cluster nazionale dual-use, come avvenuto in altri Paesi, e con quali caratteristiche – se

riconosciuto dal Ministero dell'Università e della Ricerca, privato, o di altra tipologia – e con quali mandati relativi al trasferimento tecnologico su una selezione di aree di interesse. Resta comunque opportuna e complementare anche la trattazione di tematiche dual-use all'interno dei cluster esistenti come avviene nel Cluster Tecnologico Nazionale Aerospazio. Diversi studi in passato hanno raccomandato la definizione di un database industriale europeo, relativo a tecnologie e prodotti dual-use disponibili e progetti di R&S dual-use a livello degli Stati membri e a livello UE. Una realizzazione molto complessa sia dal punto di vista politico e degli interessi industriali che tecnico, ma che ora sembra poter avere una possibilità a livello di tecnologie critiche, in larga parte dual-use. Infatti, il *Piano d'azione sulle sinergie* della Commissione prevede la creazione di un Osservatorio sulle Tecnologie Critiche che raccoglierà dati su quelle emergenti in un rapporto classificato per gli Stati membri, entro la fine del 2022, con cadenza biennale. L'Osservatorio è in via di definizione e sarà fondamentale garantire il giusto accesso all'industria.

Una governance efficace ed efficiente dei finanziamenti è fondamentale per garantire coerenza, continuità e ottimizzazione delle risorse, e può orientare in modo incisivo l'innovazione dual-use. Il quadro europeo, nonostante i progressi, resta frammentato. Alcuni ritengono sia auspicabile puntare ad un coordinamento strategico preventivo sugli investimenti in aree dual-use tra i Programmi in materia di sicurezza e in materia di difesa e che sia basato su un meccanismo strutturato e istituzionalizzato che coinvolga i Comitati di programma e la Commissione. Anche a tale proposito sarà importante l'avvio da parte della Commissione, entro la prima metà del 2022, di un incubatore di innovazione dual-use per sinergie tra i tre settori civile, difesa e spazio e tra questi ed altri ecosistemi. A livello nazionale - rispetto ai finanziamenti europei - è bene valutare, in alcuni casi, anche le sovrapposizioni, così come per le tecnologie sovrane. Sia a livello UE che a livello italiano, infine, è necessario che il settore pubblico dia adeguata visibilità alle opportunità di finanziamento dual-use e fornisca regole di ammissibilità chiare e semplici, incluse le modalità di screening dual-use nelle proposte di ricerca. Questo per facilitare l'accesso da parte di nuovi soggetti, anche del mercato inverso. Inoltre, sarebbe utile fornire supporto tecnico, gratuito o a costi contenuti, in particolare alle Piccole e Medie Imprese (PMI).

Il tema della semplificazione riguarda anche le normative. Con riferimento all'export dual-use appare utile l'armonizzazione delle applicazioni nazionali per evitare effetti distorsivi su efficacia ed efficienza del controllo delle esportazioni e sull'applicazione uniforme di embarghi, oltre che sulla concorrenza. A tale ultimo proposito, è da considerare che la compliance deve essere vista come un enabler della competitività per l'azienda. Il Ministero degli Affari Esteri e della Cooperazione Internazionale sta per introdurre un

sistema di e-licensing per la gestione completamente informatica delle autorizzazioni all'esportazione di beni e tecnologie dual-use. Con riferimento agli Intellectual Property Rights (IPRs) si deve puntare ad una definizione il più possibile univoca, accessibile, e armonizzata a livello UE per facilitare le collaborazioni. In particolare, le PMI dovrebbero essere supportate con consulenze e formazione per la gestione degli IPRs sia per bandi europei che per il trasferimento tecnologico a livello internazionale.

Per tutti i fattori descritti, quello delle definizioni e terminologie comuni si conferma un aspetto fondamentale anche per l'innovazione dual-use. Quanto alla domanda, definizioni e terminologie comuni sono indispensabili per la comprensione di esigenze, funzioni, requisiti e livelli di TRL. Quanto al monitoraggio tecnologico, favoriscono, o a volte sono condizione per, la validità di strumenti di politica tecnologica ed industriale. Quanto alla governance dei finanziamenti pubblici, e in particolare l'accesso a finanziamenti, la mancanza di riferimenti condivisi può avere impatti negativi sull'orientamento degli stakeholder pubblici e privati nei bandi di ricerca e sulla fattibilità. Quanto alle normative, la mancanza di definizioni comuni può implicare effetti distorsivi su efficacia ed efficienza del controllo delle esportazioni e sull'applicazione uniforme di embarghi, oltre che sulla concorrenza.

Per i prossimi mesi erano già previste novità rilevanti per il tema dual-use. La reazione nazionale, della UE e della NATO al conflitto russo-ucraino potrebbe influenzare la possibilità di attivare alcune delle azioni suggerite e la loro priorità. Tali sviluppi dovranno essere analizzati tenendo presente che volontà politica e fattore culturale professionale, tanto lato offerta che lato domanda, restano alla base di ogni possibile cambiamento. In assenza non vi è disposizione teorica volta a favorire l'innovazione dual-use che possa veramente funzionare.

EXECUTIVE SUMMARY (En)

At the time of writing, the role of the Armed Forces is being highly debated, amid the conflict between Russia and Ukraine which reached a phase of great intensity. The conflict's implications on the operational models of the military instrument, as well as on investments, do not yet appear clear, but will likely turn out to be profound, medium-to-long-term consequences at national, EU, and NATO level.

The current analysis aims at describing the factors influencing dual-use innovation processes, both in terms of Research and Development (R&D) and of technology and product transfer for applications in the opposite market. This goal intends to encourage the Ministry of Defence to resort to dual-use solutions, without the need to compromise any specific military capability and whilst being able to count on separate investment lines: military only on the one hand, and dual-use on the other. Chapter 1 describes the framework of the current debate, considering the difficulties in reaching commonly agreed definitions in the field of dual-use solutions, and underlining the positive implications that dual-use technologies and products can have in terms of interoperability, innovation, and funding opportunities.

Chapter 2 describes the main factors influencing both the private and the public sectors.

With respect to the former, the study draws attention to the elements that companies take into consideration when assessing the feasibility of innovative dual-use solutions and the opportunities they may provide. Such elements include the specific type of company and its possible business strategies, such as its approach to development and diversification towards clients, technologies and products belonging to the opposite market. A company's starting point in terms of strategic/traditional core business is a crucial element to take into account. The more a company drifts away from its core business, the greater is the price it will pay not just in the economical-financial realm, but also in terms of transaction costs that will be necessary to extend, adapt or acquire competences required to function in the opposite market. These competences may range from knowledge and access to financing tools, to compliances with regulatory frameworks at large concerning, for instance, exports and standards. Overall, the above-mentioned starting point – namely, whether a given company traditionally operates in the civil/security or the military sector – is very significant for its ability to overcome possible barriers to accessing the opposite market, in combination with all other elements characterising the company. For this reason, each factor is further analysed throughout the steps taken to switch from civil/security to military, and vice versa. Chapter 2 also offers a description of the main features of R&D as the context within which

a company makes decisions concerning dual-use products and technologies, including the interaction between supply and demand. The analysis ranges from open innovation to the role of technology brokering offices within companies; from technological bricks and Commercial Off-the-Shelf (COTS), to the relevance of the different Technology Readiness Levels (TRLs). The Chapter also provides concrete examples of dual-use R&D processes and technology and product transfer for applications in the opposite market.

As far as the public sector is concerned, the study outlines elements that are mainly handled by public organisations, but which do have either a direct or an indirect impact also on companies. The macro-themes taken into consideration include demand, technological know-how, the governance of public funding, and regulations.

Starting from these macro-themes, Chapter 3 analyses a few factors though which the public sector could facilitate dual-use innovation.

Public demand is pivotal for innovation. The first recommendation stemming from this study concerns the need for a comparative analysis of different procurement systems employed by administrations that may be suitable for dual-use synergies. Such effort may facilitate assessing whether it would be possible to formulate a demand based on functions for areas of interest that are compatible or common within different Ministries/entities of both the civil/security and the military sectors. This could extend the research of solutions in opposite sectors, whilst also taking into consideration open innovation models. The next step would be setting procedures for defining common/dual-use technical requirements for the areas that are believed to include compatible or shared functions among different Ministries/entities. This may also include adaptations to requirements established by central or local administrations of the opposite sector. Dual-use innovation remains directly proportional to the compatibility between standards of different sectors and the possibility to formulate hybrids standard. According to the *Action Plan on synergies between civil, defence and space industries*, by the end of 2022 the European Commission will present a Plan to promote the use of existing hybrids standard and the development of new ones. At the Italian level, experts claim that actions concerning all the themes described above should be addressed by a decisional Technical Board under the Presidency of the Council of Ministers. Such a Board would have both a political and an operational level and it would include working groups focusing on distinct issues (which, among other things, could select initial areas of dual-use interest), with specific goals and deadlines.

The knowledge about available or developing technologies and products and their potential applications is one of the most critical factors when it comes to the interaction between supply and demand in dual-use innovation. The public sector should identify the

more suitable available tools to facilitate such process and set new ones. Among the available tools, the ones that can be adapted for dual-use innovation purposes are considered to be the more interesting. They include external technology brokering offices that should function as hubs for technology transfer. They should be characterised by neutrality, like institutional entities, and they should be supported by public funding and well-integrated within the European context. As far as technological/industrial clusters are concerned, Italy should explore the possibility to create a national dual-use cluster, which other countries already have. It should then determine its distinct features – for instance, whether it would be accredited by the Ministry of University and Research, a private entity, or something else – and its mandates related to technology transfer for a selection of areas of interest. With that being said, it will be important to continue working on dual-use in the context of existing clusters, such as the National Aerospace Technology Cluster. Several studies conducted in the past recommended the creation of a European industrial database, which would include available dual-use products and technologies and R&D dual-use projects at national and EU level. Despite being a challenging goal in terms of political will, industrial interests and technical capacities, such a database could nowadays be feasible for critical technologies, which are mostly dual-use. Indeed, the European Commissions' *Action Plan on synergies* includes the creation, by the end of 2022, of an Observatory on Critical Technologies, which will gather data on emerging technologies every two years in a classified report. The Observatory is currently being developed, and it will be important to grant the industrial sector an appropriate access to the information.

An efficient and effective governance of funding is crucial to guarantee coherence, continuity, and resource optimisation, and it may significantly influence dual-use innovation. Despite the improvements that have been achieved, the European framework remains fragmented. According to some experts, it would be favourable to implement a preventive strategic coordination effort between European security and defence Programmes when it comes to investments in dual-use areas. Such effort could be based on a structured and institutionalised mechanism involving both Programme Committees and the Commission. This is yet another reason why the Commission's plan to launch, by the first half of 2022, a dual-use innovation incubator for synergies between the civil, the defence, and the space sector – and among these areas and other realms – represents an important objective. At national level, when assessing European funding opportunities, it is also relevant to positively consider the possibility of overlaps, for example in the field of sovereign technologies. Finally, both at EU and national level, it is crucial for the public sector to correctly advertise dual-use funding opportunities, providing clear-cut and simple rules of

admission, starting from dual-use screening procedures for research proposals. This may facilitate access to new entities, also belonging to the opposite market. Moreover, it may be useful to provide organisations – especially Small and Medium Enterprises (SMEs) – with technical support, either free or at a reduced price.

Simplification also concerns regulations. With respect to dual-use exports, harmonising national applications could avoid distortive effects on the effectiveness and efficiency of export control and on the uniform application of embargos, and on competition. In this regard, it should be noticed that compliance should be considered an enabler of competitiveness for a given company. The Italian Ministry of Foreign Affairs and International Cooperation is about to introduce an e-licensing system for the digital management of dual-use goods and technologies export authorisations. As far as Intellectual Property Rights (IPRs) are concerned, it is important to reach unambiguous, accessible, and harmonised definitions at EU level, in order to facilitate possible collaborations. More specifically, consultants and trainers should support SMEs with the management of their IPRs, both for European calls and the technology transfer at international level.

Definitions and common terminologies continue to represent a critical aspect for dual-use innovation for all the factors described above. As for demand, they are indispensable for the comprehension of needs, functions, requirements, and TRLs. As for technological monitoring, they promote – or are sometimes a condition for – the validity of technological and industrial policy instruments. With respect to the governance of public funding, and especially the access to funding, the lack of shared references might have negative consequences on both public and private stakeholders' ability to look for open calls for research as well as their feasibility. Lastly, the absence of common definitions might implicate distortive effects on regulations, with special regard to the efficacy and efficiency of export control and the homogeneous implementation of embargos, as well as the competition.

Although there were already new actions in place concerning dual-use in the next few months, reactions to the Russian-Ukrainian conflict at national, EU and NATO level might influence the prospective course of realisation as well as the priority scale. These developments will have to be considered bearing in mind that political will and professional cultural factors, both on the supply and on the demand side, continue to be the foundation of any possible change. Without them, there are no effective theoretical provisions able to really encourage dual-use innovation.

CAPITOLO 1 - DUAL-USE: INQUADRAMENTO E POTENZIALI VANTAGGI

INQUADRAMENTO E DEFINIZIONI

Il dibattito attorno alle tecnologie dual-use ha tradizionalmente ricevuto input di tipo accademico e di tipo governativo-istituzionale e normativo ai quali si è poi aggiunto un crescente numero di studi. Il termine "dual-use" si ritrova utilizzato in correlazione con un numero rilevante e diversificato di altri termini: dual-use applications, dual-use awareness, dual-use capabilities, dual-use concept, dual-use context, dual-use community, dual-use market, dual-use methodologies, dual-use outcomes, dual-use potential, dual-use purpose e moltissimi altri oltre a, naturalmente, dual-use technologies.

Alla vastità terminologica si accompagnano due elementi. Il primo è una non univoca definizione di quali siano le caratteristiche distintive di tecnologie e prodotti dual-use. Il secondo è la varietà di contesto di riferimento. I due elementi sono collegati perché le caratteristiche distintive variano anche in base all'ambito e alle finalità delle analisi ed entrambi restano soggetti ad interpretazioni diverse, se non anche opposte, e che evolvono nel tempo. La dualità resta un fenomeno complesso, difficile da osservare perché diversi possono essere i punti di vista: tecnologie, meccanismi di trasferimento, reti, cicli di vita della tecnologia, finanziamenti, imprese, mercati, ed altro[1]. La divisione tra caratteristiche e contesto è dunque funzionale all'esposizione del problema, ma va considerato che quanto di seguito indicato per le possibili caratteristiche distintive di tecnologie e prodotti dual-use, va sempre letto in correlazione con il contesto di analisi (influenzato appunto da fattori politici, legali, tecnici, industriali, etici, storici, etc.).

Quanto alle caratteristiche distintive di tecnologie e prodotti dual-use il problema metodologico non è solo definire il termine dual-use ("utilizzo duale"), ma anche il termine "tecnologia". E infatti il termine tecnologia può avere diverse accezioni. Alcune molto comprensive, come quella riportata dall'Enciclopedia Treccani: "Vasto settore di ricerca (la ricerca tecnologica), composto da diverse discipline che ha come oggetto l'applicazione e l'uso degli strumenti tecnici in senso lato, ossia di tutto ciò che può essere applicato alla soluzione di problemi pratici, all'ottimizzazione delle procedure, alla presa di decisioni, alla scelta di strategie finalizzate a determinati obiettivi. Il termine [...] si riferisce all'utilizzazione ottimale, anche e soprattutto da un punto di vista economico, dell'insieme di tecniche e procedimenti diversi impiegati in un dato settore e delle conoscenze tecnico-scientifiche più avanzate e, più in generale, a un insieme di elaborazioni teoriche e sistematiche, applicabili

[1] Zyla, C. e Meunier, F.X. (2014), "Empreinte de l'innovation duale sur la croissance des entreprises: l'enseignement d'une analyse structural", University of Paris Ouest, Ottobre, p. 7

globalmente alla pianificazione e alla razionalizzazione dell'intervento produttivo". Altre più limitate, come quelle che intendono la tecnologia come abilità di riconoscere e risolvere problemi tecnici[2] o come comprensiva di prodotti, conoscenze e competenze[3], oppure come l'insieme di conoscenze, capacità e manufatti utilizzati per sviluppare, produrre e consegnare prodotti e servizi[4].

Le differenze sul significato di cosa il termine tecnologia comprenda possono avere conseguenze sostanziali, perché influenzano l'attenzione degli stakeholder su specifici aspetti delle questioni in discussione e non su altri. Con implicazioni diverse a seconda ad esempio che si considerino tecnologie di prodotto o tecnologie di processo. Le interpretazioni del significato di tecnologie dual-use si differenziano anche in base alla preferenza per una dualità non focalizzata sulle caratteristiche intrinseche della tecnologia, ma sul contesto socio-tecnico che ne determina sviluppo e applicazioni. In tal senso la dualità non sarebbe tipicamente inerente alla tecnologia stessa, ma dipenderebbe dalla rete sociale, tecnica e organizzativa nella quale è sviluppata o utilizzata. Esempi di dualità focalizzata sulle caratteristiche intrinseche della tecnologia sono quelli relativi al concetto di "purpose"/"designed for" come anche nella definizione dell'Oxford Dictionary: "(Of technology or equipment) designed or suitable for both civilian and military purposes". Alcuni autori ritengono non sia sostenibile attribuire il carattere dual-use né dalle sole caratteristiche intrinseche delle tecnologie né dal solo contesto, sostenendo una reciproca influenza in cui l'interazione civile-militare condiziona le applicazioni tecnologiche e in cui molti aspetti tecnologici rilevano per l'interpretazione dell'uso di una tecnologia come militare, civile o dual-use[5].

Vi sono poi diverse posizioni sul privilegiare nell'analisi l'attualità o la potenzialità del carattere dual-use di tecnologie e prodotti. Alcuni ritengono che una tecnologia o un prodotto diventi dual-use solo nel momento in cui soddisfa esigenze civili/sicurezza e militari. La dualità sarebbe dunque acquisita, persa e riacquisita a tale condizione[6], con cambio di applicazione da un settore a quello inverso, possibile più volte nel corso del ciclo di vita di

---

2 Autio, E. e Laamanen, T. (1995), "Measurement and evaluation of technology-transfer - review of technology-transfer mechanisms and indicators", International Journal of Technology Management, p. 647

3 Te Kulve, H. e Smit, W. A. (2003), "Civilian-military co-operation strategies in developing new technologies", Research Policy, p. 957

4 Institut de Relations Internationales et Stratégiques (IRIS), IAI, Manchester Institute of Innovation Research (MIIR) (2010), "Study on the industrial implications in Europe of the blurring of dividing lines between security and defence", 15 Giugno, p. 63

5 Te Kulve, H. e Smit, W. A. (2003), "Civilian-military co-operation"

6 Mérindol, V. e Versailles, D. W. (2014), "La dualité dans les entreprises de Défense", Ministère de la Défense, Settembre, p. 17

tale tecnologia[7], e una tecnologia potenzialmente dual-use potrebbe non mostrare mai usi dual-use.

Quanto al contesto di analisi di tecnologie e prodotti dual-use, si rileva che alle tradizionali analisi in ottica di controllo, volte a contrastare eventuali usi impropri di tali tecnologie, si sono aggiunte analisi su modalità che favoriscano sinergie tra gli ambiti civile/sicurezza e militare sia a livello di ricerca e sviluppo (R&S) dual-use che di trasferimento di tecnologie e prodotti dual-use. Queste ultime sono raramente supportate da dati empirici, a causa della sensibilità di alcune informazioni di provenienza militare o industriale e generalmente descritte attraverso casi di studio e non misure quantitative per cui sarebbe più difficile costruire induzioni valide per tutti i soggetti[8].

Il risultato è una varietà di significati attribuiti al concetto dual-use presente anche in ambito istituzionale, nonostante i tentativi di definizione. Questo si verifica anche a livello dei tradizionali contesti di analisi sull'applicazione di regolamentazioni. Con un equilibrio difficile tra il rischio di definizioni troppo strette – che potrebbero lasciare fuori R&S potenzialmente soggette ad uso improprio e che quindi dovrebbero invece essere regolate – o troppo larghe – con conseguente rischio di complessi quadri amministrativi che non solo rendono inefficace o non gestibile il controllo, ma impediscono un ottimale svolgimento di attività di ricerca e innovazione[9]. Un bilanciamento non facile da stabilire ed in continua evoluzione nella relazione tra dual-use e data sharing[10], anche considerando che la ricerca non ha bisogno di essere ufficialmente designata come dual-use per esserlo[11].

Sempre per quanto riguarda il peso del tema delle definizioni, il quadro che emerge dalla letteratura, dai documenti istituzionali e dagli studi conferma che in diversi casi autori, esperti, practitioner ed istituzioni danno per scontate definizioni oggetto dei propri studi e/o danno per condivise e/o interpretabili definizioni oggetto di disposizioni normative. Secondo alcuni, da ultimo anche la Commissione europea (CE) nel suo *Piano d'azione sulle sinergie tra l'industria civile, della difesa e dello spazio*[12] ha evitato di trattare il tema definizioni per non intraprendere questioni poco risolvibili. Per inciso, dare per scontate le definizioni non sembra essere una caratteristica specifica del solo tema dual-use. Si consideri, ad esempio, il tema della cybersecurity: alcuni osservano in maniera provocatoria che, per quanto il

---

7 Molas-Gallart, J. e Sinclair, T. (1999), "From technology generation to technology transfer: the concept and reality of the Dual-Use Technology Centres", Technovation, p. 662

8 Acosta, M., Coronado, D. e Marin, R. (2011), "Potential Dual ‐ Use Of Military Technology: Does Citing Patents Shed Light On This Process?", Defence and Peace Economics

9 Resnik, D. B. (2009), "What is Dual-use Research? A Response to Miller and Selgelid", Science and Engineering Ethics, p. 4

10 Bezuidenhout, L. (2013), "Data Sharing and Dual-Use Issues", Science and Engineering Ethics, p. 84

11 Oltmann, S. (2015), "Dual-use research: investigation across multiple science disciplines", Science and Engineering Ethics, p. 7

12 CE (2021), "Piano d'azione sulle sinergie tra l'industria civile, della difesa e dello spazio", 22 febbraio

concetto sia trattato come centrale, proprio la precisa natura del problema non è ben definita, lasciando piuttosto spazio ad una combinazione di intuizione ed incertezza (mischiata a pessimismo) che può impattare negativamente sull'analisi[13]. Diversi autori ed esperti confermano che, mentre il tema del dual-use è di sicuro interesse, non esiste una definizione generalmente accettata[14]. Altri ritengono che il termine "tecnologia dual-use" venga utilizzato per descrivere molti concetti, alcuni dei quali appartengono chiaramente ad altre categorie[15]. Altri ancora criticano articoli di colleghi sostenendo che essi forniscono un'eccellente panoramica dei dilemmi etici e politici relativi alla ricerca dual-use nella biologia senza, però, fornire una chiara definizione di cosa sia "dual-use"[16].

Il problema relativo alle definizioni di dual-use si rileva anche per quelle istituzionali. A livello di Organizzazione delle Nazioni Unite (ONU), ad esempio, in un documento della World Health Organization (WHO) dal titolo *Responsible life sciences research for global health security - A guidance document* si riporta come, per quel che riguarda il concetto di ricerca dual-use, siano state avanzate varie definizioni sulle quali non si rileva un consenso comune[17]. Ancora in ambito di controllo delle armi di distruzione di massa, ad esempio, né la risoluzione 1540 (2004) del Consiglio di Sicurezza dell'ONU, né le relative risoluzioni di follow up (1673, 1810, 1977) hanno discusso e definito il concetto di dual-use[18]. Oppure, come nel caso del Codice di Condotta dei Paesi Bassi per la Biosicurezza uscito nel 2007, si usa il termine "dual-use" senza mai esplicitarne una definizione[19].

La ragione di un mancato consenso su cosa siano le tecnologie dual-use deriva, secondo alcuni, dalla varietà di tali tecnologie e dalla ancor più vasta gamma di meccanismi di trasferimento che le riguardano nello spostamento tra applicazioni civili e militari[20]. La mancanza di definizioni condivise può impattare negativamente su diversi aspetti di governance, organizzativi e gestionali. Ad esempio, in ambito controllo export dual-use, può limitare efficacia ed efficienza del controllo, dell'applicazione uniforme degli embarghi[21] e può implicare effetti distorsivi sulla concorrenza. Anche per quel che riguarda l'accesso a finanziamenti di R&S si possono avere conseguenze come nel caso in cui, in assenza di

---

13 Cornish, P., Hughes, R. e Livingstone, D. (2009), "Cyberspace and the National Security of the United Kingdom Threats and Responses", Chatham House Report, Marzo, p. 1
14 Forge, J. (2010), "A Note on the Definition of Dual-use", Science and Engineering Ethics, p. 1
15 Bailey, R. (1993), "Dual-use Technology: Status, Issues and Change", National Defence University
16 Resnik, D. B. (2009), "What is Dual-use Research?", p. 1
17 World Health Organization (2010), "Responsible life sciences research for global health security. A Guidance Document", WHO Document Production Services, p. 8
18 Rath, J., Ischi, M. e Perkins, D. (2014), "Evolution of different Dual-use concepts in International and National Law and its implications on Research Ethics and Governance", Science and Engineering Ethics
19 Ivi, p. 10
20 Molas-Gallart, J. (1997), "Which way to go? Defence technology and the diversity of 'dual-use' technology transfer", Research Policy
21 Rath, J., Ischi, M. e Perkins, D. (2014), "Evolution of different Dual-use concepts"

indicazioni chiare e condivise, ad esempio nell'ambito dell'Unione Europea (UE), si lasci al singolo valutatore di proposte di progetto la responsabilità di decidere quali contenuti siano effettivamente relativi a tecnologie dual-use al fine di valutarne la ammissibilità al bando.

La questione della definizione delle tecnologie dual-use resta dunque di non facile risoluzione. Resta anzi aperta e soggetta ad evoluzioni delle interpretazioni. Premettendo quindi che il termine tecnologia è vasto ed include concetti che vanno dalla ricerca e conoscenza codificata e know-how ai servizi e al software, dalle tecnologie di prodotto e componenti alle tecnologie di processo, si propone una definizione che prende in considerazione le caratteristiche principali rilevate nelle fonti e tra i practitioner: una tecnologia può essere considerata dual-use, quando può avere duplice applicazione/uso negli ambiti civile/sicurezza e militare. Al dual-use si arriva attraverso un processo di R&S che dà luogo ad una tecnologia progettata ab initio come dual-use oppure tramite trasferimento da un ambito all'altro (con o senza adattamento) durante l'intero ciclo di vita della tecnologia.

R&S e trasferimento tecnologico sono entrambi strumenti per l'innovazione dual-use. Con il primo si possono identificare le attività realizzate ex novo e con il secondo quelle in cui le attività partono da tecnologie e prodotti sviluppati (o in via di sviluppo nella scala di maturità tecnologica) a fini civili/sicurezza o militari e vengano poi estese ad applicazioni del mercato inverso. Le fonti, numerose per quel che riguarda le tematiche di R&S e trasferimento tecnologico, risultano invece più limitate sugli specifici argomenti R&S dual-use e trasferimento di tecnologie e prodotti dual-use. R&S e trasferimento tecnologico sono stati trattati da alcuni autori in chiave dual-use anche in maniera collegata, per cui non è agevole distinguere quelli maggiormente focalizzati sul primo concetto rispetto a quelli maggiormente focalizzati sul secondo.

Inoltre, la maggior parte delle innovazioni non è determinata dalla scoperta di qualcosa di fondamentale, nuovo o originale, ma è il risultato di nuove combinazioni di concetti e materiali già conosciuti[22]. Questo implica, anche per l'ambito dello sviluppo e della diffusione di tecnologie e prodotti dual-use, la ricerca di un diverso modo di operare alla frontiera dei differenti ecosistemi degli ambiti civile/sicurezza e militare. Le differenze che ostacolano una possibile dualità tra i settori civile/sicurezza e militare non dipendono, o non dipendono solo, dalle caratteristiche intrinseche della tecnologia, ma dalle strutture organizzative, dagli approcci degli stakeholder protagonisti dell'innovazione e dal loro modo di interagire sia nelle fasi di R&S che nell'intero ciclo di vita della tecnologia in un contesto di policies,

[22] Tonchia, S. e Nonino, F. (2007), "La Guida del Sole 24 Ore al Project Management. Gestire l'innovazione nei prodotti e nei servizi", Il Sole 24 Ore

normative, regolamenti e disposizioni contrattuali che influiscono sui processi di innovazione più del solo aspetto tecnologico[23].

OBIETTIVO DELLA RICERCA E POTENZIALI VANTAGGI DEL DUAL-USE

Il potenziale dual-use è più una questione di organizzazione e di governance dell'innovazione che un problema puramente tecnologico[24]: interpretazioni inizialmente basate solo su variabili tecnologiche vengono quindi estese a variabili di tipo organizzativo e gestionale, sia in ambito aziendale che di organizzazioni pubbliche. Diversi autori dunque cercano di astrarsi, per quanto possibile, dal livello del problema di definizione dell'oggetto "tecnologie dual-use", studiando il quadro degli aspetti organizzativi e gestionali del processo di innovazione dual-use. Alcuni, nell'affrontare il tema del trasferimento delle tecnologie dual-use, focalizzano l'analisi più sugli aspetti organizzativi che regolano le relazioni tra tecnologie civili/sicurezza e difesa che sulle tecnologie stesse. Altri definiscono il dual-use come una modalità di gestione della ricerca, dell'innovazione e della produzione di sistemi di difesa volta a generare forme di economicità e spillover con il settore civile/sicurezza. Altri ancora studiano le condizioni organizzative ed informative per realizzare il potenziale dual-use.

Lo studio segue tale impostazione proprio al fine di descrivere dinamiche quanto più possibile indipendenti dalla tipologia di tecnologia o prodotto dual-use oggetto di R&S o di trasferimento. L'obiettivo principale è determinare l'influenza di fattori organizzativi e gestionali sui processi di innovazione dual-use, sia a livello di R&S dual-use che di trasferimento di tecnologie e prodotti dual-use. Tali aspetti determinano infatti, insieme alle (e talvolta più delle) caratteristiche intrinseche di tecnologie e prodotti, la possibilità di realizzare il potenziale dual-use nei vari livelli di maturità tecnologica. Il risultato dell'esercizio intende fornire strumenti di supporto alle organizzazioni pubbliche e alle aziende per capire come strutturare aspetti organizzativi e gestionali al fine di guidare l'innovazione dual-use.

Nonostante una non univoca definizione di quali siano le caratteristiche distintive delle tecnologie dual-use, spesso anche all'interno della stessa tipologia di stakeholder, si registra un interesse crescente per il tema. I motivi sono diversi, e nel contesto europeo sono riconducibili ad alcuni driver principali tra cui sinergie operative civili-militari, innovazione e competitività industriale e finanziamenti in R&S, come di seguito analizzati.

---

[23] Evans, S. A. (2006), "Defining Dual-Use: An international assessment of the discourses around technology", WMD Proliferation Seminar Series, 27 Febbraio, p.3

[24] Mérindol, V. e Versailles, D. W. (2014), "La dualité dans les entreprises de Défense", p. 17

INTEROPERABILITA'

La Difesa italiana riconosce il potenziale contributo che tecnologie e prodotti dual-use potrebbero fornire in termini di interoperabilità. La disponibilità di strumenti dual-use, soprattutto se *secure-by-design*, è stata individuata quale fattore abilitante della Capacità Operativa Fondamentale Comando, Controllo e Consultazione delle Forze Armate (FFAA). Tali strumenti infatti sono in grado di garantire l'interoperabilità a livello interforze, NATO/UE e di coalizione, ma anche verso Ministeri, autorità, agenzie ed enti del settore pubblico e privato[25]. L'interoperabilità intersettoriale derivante dall'impiego di tecnologie e prodotti dual-use permette di aumentare l'efficacia delle operazioni anche sulla base di addestramenti comuni e condivisione di informazioni, favorendo l'ottenimento di una "picture" comune nell'intero di ciclo di gestione della minaccia.

Le aree in cui ha più senso realizzare un'interoperabilità sono quelle in cui sono possibili requisiti tecnici comuni/dual-use per applicazioni high-end civili/sicurezza e low-end militari. Mentre in missioni ad alta intensità di conflitto il fattore interoperabilità è trascurabile e l'uso di assetti dual-use ridotto, in missioni di stabilizzazione o gestione delle crisi la componente civile ricopre un ruolo più considerevole e l'interoperabilità può diventare fondamentale. È questo, ad esempio, il caso delle missioni UE in cui l'Italia è impegnata o di operazioni sul suolo nazionale per la risposta a disastri naturali, minacce ibride, o altri fenomeni di rilievo per la resilienza del Paese (e dunque dell'UE e della NATO). Ciò è particolarmente vero in termini di sistemi di comando e controllo e comunicazioni (C3), pianificazione, logistica, e Information Communication Technologies (ICTs). In tal senso, la Difesa è impegnata nell'elaborazione di un "doppio uso sistemico" delle proprie capacità tramite lo sviluppo di un apparato militare, inteso come risorse sia umane che materiali, in grado di integrarsi al meglio con la componente civile/sicurezza[26].

Secondo la stessa logica, se dal punto di vista capacitivo "combat" la componente dual-use è ridotta o inesistente (si pensi, ad esempio, ad armamenti inseriti in piattaforme complesse quali missili o carri da combattimento), per altri assetti può ricoprire un ruolo rilevante. È il caso, ad esempio, di mezzi di trasporto come elicotteri o alcune classi di navi e sistemi spaziali, dai lanciatori ai satelliti, dotati di tecnologie per l'osservazione terrestre ottiche – iperspettrali o radar – come nel caso della costellazione COSMO-SkyMed – il cui quinto satellite (il secondo della Second Generation) è stato lanciato dal Kennedy Space Center nel febbraio 2022. Il Sistema Italiano per Comunicazioni Riservate e ALlarmi

---

[25] MDIF (2021), "Documento programmatico pluriennale della difesa per il triennio 2021-2023"

[26] MDIF (2018), "Duplice uso e Resilienza. Documento di integrazione concettuale delle linee programmatiche del dicastero"

(SICRAL) sviluppato da Telespazio e Thales Alenia Space Italia è infatti un esempio di prodotto che, garantendo l'interoperabilità tra le reti militari e della sfera civile/sicurezza, comporta vantaggi significativi per entrambi i settori, assicurando servizi di comunicazione tattica e strategica.

Il raggiungimento di un più alto livello di interoperabilità dovrebbe favorire un miglioramento delle rispettive prestazioni operative. La maggior parte delle attività che si svolgono nello spazio aereo, ad esempio, sono condotte grazie alla collaborazione tra i settori civile/sicurezza e militare[27], e l'interoperabilità delle tecnologie alla base delle infrastrutture di comunicazione, navigazione e sorveglianza e di gestione del traffico aereo assicura maggiori livelli di sicurezza delle stesse[28]. Lo stesso discorso si applica all'azione comune tra FFAA, Forze dell'Ordine[29] e sistema di Protezione Civile. A titolo esemplificativo, l'Esercito è stato coinvolto in una doppia esercitazione dei reparti alpini con la Protezione Civile dall'Associazione Nazionale Alpini, tenutasi nel 2019, per testare le capacità di intervento comuni in contesti di emergenze quali alluvioni, terremoti e incendi boschivi. L'anno precedente, all'esercitazione Various Disaster Relief Management Exercise (VARDIREX) hanno partecipato Esercito, Aeronautica e Protezione Civile per testare le capacità di interoperabilità.

A livello sovranazionale, come nel caso di NATO e UE, garantire interoperabilità tra settori permette un generale miglioramento della reciproca efficienza operativa. L'Alleanza Atlantica incentiva il raggiungimento di più alti livelli di interoperabilità tra civile/sicurezza e militare, ad esempio, favorendo l'adozione e l'utilizzo di standard civili, in alcuni settori selezionati, come preferibili quando non siano strettamente necessari quelli militari[30]. Nel framework europeo, tramite il suo *Piano d'azione sulle sinergie*, la CE si è impegnata nella promozione di approcci comuni ai settori civile/sicurezza e militare al fine di migliorare il processo di individuazione di esigenze e rispettive soluzioni – un obiettivo da conseguire attraverso l'Azione 1. Da considerare, infine, che l'interoperabilità è anche volta all'incremento delle capacità di azione esterna dell'Unione e dell'indipendenza tecnologica europea.

L'interoperabilità può essere perseguita tramite tecnologie e prodotti dual-use, ma deve, inoltre, esserlo tramite i relativi quadri organizzativi, logistici, procedurali e legali –

---

27 EUROCONTROL (2020), "Civil-military CNS Interoperability Roadmap", p. 17,

28 Taylor, A. A. e Ogutu, K. (2021), "ICAO Civil Military Cooperation Manual", Virtual Workshop on the implementation of an effective Civil – Military Cooperation, Aprile

29 Si veda: MDIF "Pubbliche calamità - Esercito Italiano"; e Ministro per i rapporti con il Parlamento (2020), "Contributo alla sicurezza nazionale", in «Relazione sullo stato della disciplina militare e sullo stato dell'organizzazione delle Forze Armate», Senato della Repubblica, 3 dicembre, pp. 94-101

30 Lapsley, S. (2018), "NATO use of Civil Standards", International Standardization Workshop, Ottobre

anche questi, conseguentemente, potenzialmente oggetto di innovazione dual-use. L'interoperabilità può favorire la definizione di esigenze operative e requisiti comuni ad entrambi i settori, incentivando una domanda comune di soddisfacimento delle funzioni associate a tali esigenze operative. Se da un lato dunque il dual-use può permettere di soddisfare esigenze e requisiti di interoperabilità, questa a sua volta favorisce l'emergere di soluzioni dual-use. L'interoperabilità costituisce un driver industriale con un impatto diretto sul processo di innovazione tecnologica e i rispettivi meccanismi di finanziamento.

INNOVAZIONE

Lo European Innovation Scoreboard[31] viene pubblicato annualmente dalla CE. Tra il 2014 e il 2021, l'UE ha registrato una crescita nelle prestazioni di innovazione, con un incremento totale del 12.5%. L'UE risulta migliore di attori internazionali quali Cina, India, Russia e Sudafrica, mentre altri mantengono un vantaggio rispetto all'Unione – è il caso di Corea del Sud, Canada, Australia, Stati Uniti e Giappone. L'Italia rientra tra i cinque Stati membri che hanno registrato il maggiore incremento in termini di innovazione nel lasso di tempo considerato (insieme a Cipro, Estonia, Grecia, e Lituania), con una crescita del proprio indice di innovazione del 25% tra il 2014 e il 2021.

Tuttavia il rendimento italiano continua ad essere inferiore rispetto alla media europea. L'Italia rientra infatti nella categoria degli "innovatori moderati", vale a dire dopo "leader dell'innovazione" e "innovatori forti" e prima di "innovatori emergenti". Gli indicatori italiani presentano, inoltre, sviluppi eterogenei suggerendo che, nonostante il Paese segua complessivamente una traiettoria diretta all'innovazione, continui ad essere carente sotto alcuni aspetti. Infatti, se alcuni indicatori registrano crescite, altri si mantengono stabili e altri sembrano addirittura diminuire. Ad esempio, l'indicatore *direct government funding and government tax support for business R&D* ha visto un incremento di 0.598, a fronte del dato non incoraggiante su *R&D expenditure in the public sector*, diminuito di 0.033.

Se in passato erano piuttosto attori statali, o enti ad essi associati, a guidare l'evoluzione tecnologica, oggi sono in maniera crescente piccole e medie imprese (PMI) e start-up. Questo implica che la Difesa dipende sempre più anche da tecnologie che vengono sviluppate nell'ambito del settore civile/sicurezza[32]. L'innovazione civile/sicurezza infatti, in determinati ambiti alimenta quella militare, invertendo il tradizionale trend inverso (si pensi all'invenzione di Internet). Ciò è particolarmente vero per tecnologie caratterizzate da ritmi

---

31 CE (2021), "European Innovation Scoreboard 2021"

32 Leonardo Company, "The Italian aerospace, defence and security industry. How to create industrial development, new technological capabilities and economic growth for the country"

di sviluppo e innovazione rapidi. Questo ovviamente avviene solo in determinati ambiti. In altri resta infatti fermo che alcune esigenze specifiche di assetti militari altamente performanti spingono in maniera decisiva l'innovazione, rappresentando ancora oggi un forte driver per l'innovazione tecnologica[33]. Come rimarcato dal Ministro della Difesa, anche le FFAA sono chiamate ad esprimere una capacità di innovazione[34]. Il Concetto Strategico del Capo di Stato Maggiore della Difesa, del 2020, sottolinea la necessità di perseguire uno sviluppo capacitivo sostenibile ed orientato all'innovazione tecnologica e all'integrazione, con interazione costante tra FFAA e comparto industriale e civile[35]. In tal senso, secondo alcuni esperti il dual-use anche per la Difesa può comportare dei vantaggi: su tecnologie commerciali già sviluppate per il mercato civile, per la possibilità di fare scouting, selezione e "customizzazione" con accorciamento dei tempi di progettazione e sviluppo e contenimento dei costi; su tecnologie da sviluppare o in corso di sviluppo, per la possibilità di condivisione delle risorse disponibili tra il mondo civile e quello della Difesa, soprattutto a quei livelli iniziali di TRL in cui la tecnologia è ancora multipurpose.

Ricerca e innovazione rafforzano la resilienza dei membri dell'UE in termini di produttività, competitività, e trasformazione economica e tecnologica. Riconoscendo la fondamentale rilevanza dei settori civile/sicurezza e militare nell'innovazione tecnologica, l'UE ha incoraggiato governi e FFAA degli Stati membri, oltre alle stesse istituzioni europee, ad esplorare modalità per ampliare e consolidare il loro rapporto con l'industria della difesa, al fine di costruire nuove e più solide sinergie tra i settori verso un maggiore sviluppo e impiego di tecnologie dual-use[36]. Dal punto di vista industriale, le sinergie tra i settori civile/sicurezza e militare potrebbero in parte contrastare la frammentazione tra le aziende operanti in tali settori, favorendo al contempo l'innovazione[37].

Nel perseguire le Azioni 4 e 6 del suo *Piano d'azione sulle sinergie*, la CE è impegnata nell'elaborazione di roadmap per stimolare l'innovazione tecnologica e promuovere la collaborazione transfrontaliera e intersettoriale, e nell'istituzione di un incubatore di innovazione per sostenere le nuove tecnologie e l'innovazione dual-use[38]. Nel settembre 2021, rappresentanti di CE, Parlamento Europeo (PE) e Consiglio dell'UE hanno firmato una Lettera di Intenti impegnandosi a produrre, nel primo quadrimestre 2022, una roadmap

---

33 Nones, M. (2014), "intervento durante la conferenza: Gli elicotteri duali nel campo della sicurezza e difesa", IAI, Ottobre

34 MDIF (2019), "Audizione del Ministro della Difesa sulle linee programmatiche del suo Dicastero presso le Commissioni Difesa congiunte della Camera dei Deputati e del Senato della Repubblica", ottobre

35 MDIF, "Concetto Strategico del Capo di Stato Maggiore della Difesa, conclusioni"

36 Bellasio, J., Slapakova, L., Huxtable, L., Black, J., Ogden, T. e Dawaele, L. (2021), "Innovative technologies shaping the 2040 battlefield", PE, Agosto, pp. 58-59

37 CE (2021), "Piano d'azione sulle sinergie"

38 Ibid.

sulle tecnologie per la sicurezza e la difesa al fine di promuovere la ricerca, lo sviluppo tecnologico e l'innovazione e ridurre la dipendenza strategica dell'UE relativamente a tecnologie critiche nei settori civile, difesa e spazio[39]. Nel febbraio 2022 la CE ha reso noto che, a tal fine, sarà istituito un Osservatorio sulle Tecnologie Critiche[40].

Nel contesto della European Defence Agency (EDA) è da segnalare il progetto ANDES (ANalysis of Dual-usE Synergies), mirato all'analisi dell'attuale scenario della politica europea sul dual-use e relativi sviluppi tecnologici finanziati dall'Unione[41]. Insieme alle attività di R&S, il trasferimento tecnologico rappresenta uno dei più efficaci strumenti di innovazione e ANDES intende facilitare proprio la creazione di un Dual-Use Technology Transfer Mechanism (DUT2M) che includa i principali attori istituzionali europei che operano nell'ambito della difesa quali EDA e CE, oltre ad altri extra-UE che collaborano con l'Unione. I risultati sono attesi entro la fine del primo semestre 2022 ed alcuni, se approvati dall'EDA Management Board, potrebbero essere resi pubblici.

Nel framework dell'Alleanza Atlantica vi sono iniziative volte all'innovazione dual-use. Ad esempio, nel 2016 è stato avviato il NATO Innovation Network: una federazione di enti interni o associati all'Alleanza entro cui opera il NATO Innovation Hub, dedicato all'utilizzo e promozione di modelli di open innovation tra gli Alleati[42] con il coinvolgimento anche di università, industrie e science and technology provider. Nel 2020, la NATO ha avviato il progetto DIANA (Defence Innovation Accelerator of the North Atlantic), con l'intento di più solide collaborazioni tra i settori civile/sicurezza e militare soprattutto riguardo start-up e PMI[43]. Una volta raggiunta la piena capacità operativa, DIANA offrirà a tutti gli Alleati e ai rispettivi comparti industriali una piattaforma che supporti la cooperazione transatlantica nello sviluppo di tecnologie critiche, promuovendo l'interoperabilità e sfruttando il potenziale dell'innovazione civile e dual-use. Il progetto intende consolidare il dialogo tra NATO ed industria già sperimentato nel contesto del NATO Industry Forum, sede del dialogo strategico tra industrie e NATO in materia di pianificazione e sviluppo. Nel Gennaio 2022, l'Italia ha candidato Torino per ospitare il Regional Office europeo di DIANA, proponendone la sede presso la Città dell'Aerospazio attualmente in fase di realizzazione – una scelta che garantirebbe un osservatorio privilegiato in ambito NATO. DIANA infatti sarà composto da due Regional Offices, nel Nord America ed in Europa, aperti ed accessibili, senza particolari

---

39 PE (2021) "Action plan on synergies between civil, defence and space industries", Legislative Train Schedule CE (2021), "Commission work programme 2022", Ottobre, p. 7

40 CE (2022), "Tabella di marcia relativa alle tecnologie critiche per la sicurezza e la difesa", 15 Febbraio

41 EDA (2021), "Promoting Technological Civil-Military Synergies", Marzo

42 Da Deppo, S. (2020), "The NATO Innovation Network", Innovation Hub, novembre

43 Finabel (2021), "Defence Innovation Accelerator for the North Atlantic (DIANA)", Agosto

requisiti di riservatezza. La decisione è attesa per la fine del mese di aprile 2022. La candidatura di Torino ha un forte supporto istituzionale ed industriale italiano che coinvolge da vicino il Distretto Aerospaziale del Piemonte (DAP) e si basa sia sull'esistenza nella città e nella regione di una filiera aerospaziale completa, che include anche attività di esplorazione spaziale, sia sulla storica attività torinese incentrata sull'aeronautica e sul volo. In particolare, il progetto della Città dell'Aerospazio nasce per sviluppare un hub tecnologico in una vasta area di R&S dove sono già presenti attori industriali come Leonardo, Thales Alenia Space, Altec, Avio Aereo, il DAP, ma anche l'ESA Business Incubation Centre (BIC), il Politecnico e altre due università pubbliche – con i rispettivi incubatori e laboratori di ricerca e sperimentazione, un'area aeroportuale consona a progetti di sviluppo di laboratori e test centres in coordinamento con l'Ente nazionale per l'aviazione civile (ENAC) e il Consiglio Nazionale delle Ricerche (CNR). L'area è anche ricca di PMI (350 a livello regionale) ad alto tasso tecnologico che hanno un business aerospaziale, ma forte anche della presenza di PMI dell'automotive ed altri settori che guardano allo spazio con crescente interesse.

FINANZIAMENTI

La dualità, come visto, può avere diverse accezioni. Ad esempio, mentre con "dualità di applicazione" si intende l'utilizzo della medesima tecnologia, componente o piattaforma per usi in ambito civile/sicurezza o militare, l'espressione "dualità di design" fa riferimento ad un processo di sviluppo e innovazione che ha inizio già nelle fasi concettuali di ideazione di un prodotto. Generalmente, i settori civile/sicurezza e militare hanno differenti priorità di investimento. Da un lato le FFAA, e la Difesa in generale, sono particolarmente attente alla dualità di applicazione – per esempio, alla Difesa interessa che i sistemi che forniscono comunicazioni satellitari abbiano un segnale di comunicazione protetto e criptato nonché uno commerciale, così da poter comunicare con le FFAA in modo sicuro. Dall'altro, il comparto industriale, così come la classe politica, predilige la dualità di design.

L'innovazione tecnologica dipende in larga parte dai finanziamenti disponibili, sia pubblici che privati. In Italia, gli investimenti pubblici nel settore della difesa e innovazione difesa sono divisi fra il Ministero della Difesa (MDIF) e il Ministero dello Sviluppo Economico (MiSE). Il MDIF, in particolare, eroga tra i 2 e i 2.5 miliardi di euro all'anno in appalti che includono attività di ricerca e tecnologia (R&T)[44]. Il Piano Nazionale della Ricerca Militare (PNRM)[45] è lo strumento del MDIF per erogare fondi R&T non associati ad appalti specifici.

---

44 Marrone, A. e Gilli, A. (2020), "Defence Innovation: New models and procurement implications. The Italian Case", Armament Industry European Research Group (ARES Group), IRIS, Ottobre

45 Si veda: MDIF, "La Ricerca & Innovazione", Difesa.it

Anch'esso dispone di un budget limitato con un'erogazione di circa 48 milioni di euro sia per il 2021 che per il 2022, e circa 40 milioni per il 2023[46]. Negli ultimi anni, il budget della Difesa italiana è rimasto quasi invariato, salvo una sensibile diminuzione dei fondi dedicati ad attività di R&T. Ciò è dovuto, in parte, alla decisione di includere finanziamenti distintamente indirizzati a progetti di R&T in più ampi programmi di equipaggiamento nei domini terrestre, navale e aereo, collegando così tali progetti allo sviluppo di prodotti e tecnologie specifiche.

Tale riduzione dei finanziamenti pone l'Italia (quindi l'UE e la NATO) in una situazione in cui la Difesa non può più dipendere esclusivamente dai fondi specifici a disposizione, ma deve dipendere anche da una comunità di innovatori appartenenti sia al settore civile/sicurezza che a quello militare, in rapporto sinergico tra loro, e capaci di sostenere uno sviluppo tecnologico potenziato ed economicamente efficiente[47]. Se confrontati con quelli pubblici, infatti, gli investimenti effettuati dal settore industriale privato offrono maggiori possibilità per la ricerca – nonostante negli ultimi anni si sia registrata una graduale riduzione degli investimenti nell'industria della difesa da parte di fondi d'investimento privati e di banche[48]. Per la Difesa, il dual-use rappresenta dunque una risorsa fondamentale in quanto permette di beneficiare di innovazioni tecnologiche non finanziate dal mondo militare. A dimostrazione di ciò, basti pensare che l'F-35 è stato l'ultimo veicolo da combattimento per cui gli Stati Uniti hanno richiesto lo sviluppo di un software all'industria della difesa. Da allora, i software sono stati sviluppati da aziende civili e poi utilizzati in ambito militare, ed è probabile che in futuro tale tendenza andrà consolidandosi proprio per la maggiore velocità dell'innovazione e per i maggiori investimenti in ambito civile.

Grazie ai rispettivi programmi di procurement multinazionali, NATO e UE ricoprono un ruolo fondamentale nel processo di innovazione tecnologica, rafforzando a loro volta la competitività della base industriale della difesa nazionale. La NATO, ad esempio, renderà operativo, entro il 2023, un Fondo per l'Innovazione diretto ad aziende specializzate in sistemi e tecnologie dual-use[49] per investimenti fino ad un miliardo di dollari in 15 anni[50]. I Paesi coinvolti sono Belgio, Repubblica Ceca, Estonia, Germania, Grecia, Italia, Lettonia, Lituania, Lussemburgo, Paesi Bassi, Polonia, Portogallo, Regno Unito, Romania, Slovacchia, Slovenia, Ungheria.

Nel 2020, i 26 Stati membri dell'EDA hanno impiegato il 17% del proprio budget per la Difesa in attività di R&S, per un investimento totale di circa 8 miliardi di euro – un dato

---

46 MDIF (2021), "Documento programmatico pluriennale della difesa per il triennio 2021-2023", p.136
47 Murray, R. (2020), "NATO Review - Building a Resilient Innovation Pipeline for the Alliance", NATO Review, Settembre
48 EDA (2021), "Pushing limits. Defence innovation in a high-tech world"
49 NATO (2021), "NATO Allies Take the Lead on the Development of NATO's Innovation Fund", Ottobre
50 Zorloni, L. (2021), "La Nato va a caccia di startup militari contro Cina e Russia", Wired Italia, Giugno

incoraggiante considerato che, nel 2019 erano stati investiti 7 miliardi e nel 2014, 4 miliardi[51]. Considerando gli investimenti privati europei in R&S nel settore della difesa e dell'aerospazio si rileva, invece, come tra il 2011 e il 2020 questi siano passati da 7 a 6.2 miliardi di euro[52.] Solo tra il 2019 e il 2020, il decremento è stato di oltre il 20%, in parte anche a causa della crisi provocata dalla pandemia di Covid-19. Per quanto concerne invece i finanziamenti per attività R&T, i 26 hanno investito circa 2.5 miliardi nel 2020 – un incremento significativo se confrontato agli anni precedenti. Tale quota rappresenta, però, solo poco più dell'1% del budget totale investito nella difesa europea.

Componenti chiave del framework UE che possono favorire tecnologie e prodotti dual-use restano i programmi quadro pluriennali di ricerca e innovazione. Già da Horizon 2020 (H2020), l'approccio è stato quello di stabilire che, pur finanziando attività di ricerca con applicazioni esclusivamente civili, si faceva espresso riferimento allo sviluppo di tecnologie dual-use, predisponendo un rafforzamento del coordinamento tra CE e EDA. H2020 ha in particolare stanziato 13,557 miliardi di euro (17.6% del budget totale) per il filone Leadership in Enabling and Industrial Technologies che include sei categorie di Key Enabling Technologies (KETs): nanotecnologia, micro e nanoelettronica (compresi i semiconduttori), fotonica, materiali avanzati, biotecnologia, tecnologie avanzate di produzione. Le KETs individuate dalla CE, sulla base delle tendenze della ricerca e del mercato a livello mondiale, restano rilevanti strategicamente per le industrie europee per il loro potenziale economico, il loro contributo alla soluzione di sfide sociali e per la loro intensità di conoscenza, e sono individuate dalla CE come ambiti di elezione per sviluppi e applicazioni dual-use. Considerando Horizon Europe, 15,348 miliardi di euro (16% del budget totale) sono dedicati ad attività di ricerca e innovazione che rientrano nel cluster Digital, Industry and Space e 1.6 miliardi per il cluster Civil Security for Society. Questi programmi di finanziamento sono accessibili anche alle industrie che producono prodotti e tecnologie dual-use[53] e sono considerati necessari per incentivare la creazione di consorzi e proteggere gli investimenti in R&T da eventuali tagli dei budget nazionali[54]. Infine il programma European Defence Fund (EDF) contenuto in Horizon Europe prevede risorse per R&S in ambito militare, per 8 miliardi di euro nel periodo 2021-2027[55].

---

51 Si veda: EDA (2021), "Defence Data 2019-2020"

52 Si veda: CE (2021), "The 2021 EU industrial R&D investment Scoreboard", JRC

53 Europe Economics (2014), "Enhancing support to SMEs - Through better understanding of dual-use aspects of the EDTIB supply chain", Novembre

54 Marrone, A. e Gilli, A. (2020), "Defence Innovation"

55 Si veda: CE, "Horizon Europe"; CE, "The European Defence Fund (EDF)"

Non sono disponibili dati ufficiali sulla specifica allocazione di fatto su dual-use nei programmi pluriennali UE di finanziamento della R&S, ma le stime ufficiali e non ufficiali spaziano da circa un terzo a circa la metà dei fondi sin dal Quinto Programma Quadro. Questi fondi costituiscono, dunque, un'importante potenziale fonte di finanziamento per grandi aziende, PMI, università e centri di ricerca operanti in ambito civile/sicurezza e in ambito militare, tanto più di interesse in un contesto variabile dei bilanci pubblici per R&S osservabile nella media dei Paesi membri UE.

Affinché tale potenziale venga propriamente utilizzato la CE ha inserito, tra le Azioni del proprio *Piano d'azione sulle sinergie,* l'obiettivo di facilitare l'accesso delle industrie che lavorano nei settori civile/sicurezza e militare ai finanziamenti disponibili per aderire ai work programme 2022, al fine di incoraggiare la partecipazione di start-up, PMI e Research and Technology Organisations (RTOs), soprattutto se attive nel campo delle disruptive technologies[56]. Il Piano, avviato nell'ambito della *Strategia industriale per l'Europa*[57], si basa su tre pilastri: sinergie, spin-off e spin-in. Le sinergie consistono in iniziative comuni tra i settori civile, difesa e spazio tramite le quali è possibile ottimizzare gli investimenti e quindi i risultati dell'Unione. Spin-off e spin-in rappresentano invece il risultato di finanziamenti dell'UE in attività di R&S: gli spin-off derivano da investimenti nei settori della difesa e dello spazio con potenziali benefici economici identificabili in sistemi e tecnologie quali la fibra ottica, Galileo e Copernicus; gli spin-in si riferiscono alle numerose potenzialità che tecnologie sviluppate nel settore civile/sicurezza quali l'intelligenza artificiale, il cloud e la robotica di cui il settore militare potrebbe beneficiare.

A livello italiano anche la *Direttiva per la politica industriale della Difesa* ha indicato la necessità di sviluppare collaborazioni tra il settore militare e quello civile/sicurezza, includendo programmi di carattere europeo e internazionale[58].

---

56 CE (2021), "Piano d'azione sulle sinergie"

57 CE (2021), "Quadro europeo di valutazione dell'innovazione", comunicato stampa, 21 Giugno; Si veda: CE (2021), "Aggiornamento della nuova strategia industriale 2020: costruire un mercato unico più forte per la ripresa dell'Europa", 5 Maggio

58 MDIF (2021), "Direttiva per la politica industriale della Difesa"

CAPITOLO 2 - FATTORI CHE INFLUENZANO L'INNOVAZIONE DUAL-USE

Analizzando i fattori che influenzano l'innovazione dual-use, sono necessarie alcune premesse. La prima è relativa alla scelta, nell'analisi dei fattori, di cercare di astrarsi da tecnologie e prodotti specifici. Come già riportato, si tratta di una scelta di metodo volta ad una maggiore generalizzazione dei risultati e delle raccomandazioni e supportata da posizioni analoghe presenti in numerose fonti. Ciò può implicare un certo grado di semplificazione nei casi in cui la natura dell'oggetto dei processi di R&S e/o di trasferimento potrebbe influenzare i processi in questione, che in alcuni casi sono più orientati al prodotto, in altri al processo e che, in particolare in settori ad alta tecnologia, possono risultare particolarmente difficili da separare. Va comunque tenuto presente che il problema dell'accesso delle aziende civili (o in generale nuove) al mercato della difesa è tipicamente connesso alla difficoltà di accesso al mondo della difesa (e di comprensione delle sue peculiarità), più che ad una questione tecnologica.

La seconda premessa riguarda la divisione dei fattori tra settore privato e pubblico, in tal modo cercando di coprire gli ambiti principali del mercato. Come infatti sostenuto da alcuni autori, tanto i fattori micro che macroeconomici determinano l'emergenza di tecnologie dual-use. Infatti, da un punto di vista aziendale, le caratteristiche e le competenze tecnologiche delle imprese hanno un peso. Come pure hanno un peso il quadro giuridico, la struttura produttiva e la tradizione industriale di una realtà nazionale[59]. Esiste tuttavia un certo grado di necessaria semplificazione nel fatto che le categorie azienda e organizzazione pubblica possono essere molto eterogenee al loro interno. Azienda, ad esempio, può essere una PMI o una corporate, un'università o un'impresa pubblica o privata, nazionale italiana o transnazionale, del settore della difesa o meno (civile, sicurezza, spazio). Organizzazione pubblica può essere un Ministero o altro tipo di agenzia che acquisisce assetti,come il MDIF e il Ministero dell'Interno (MINT) , ma anche un finanziatore di ricerca come il Ministero dell'Università e della Ricerca (MUR), senza responsabilità nella definizione di requisiti nel processo di procurement.

Come detto, l'analisi dei fattori cerca di astrarsi da tecnologie e prodotti specifici. Può essere comunque utile indicare alcuni esempi di tecnologie e prodotti dual-use. Le Categorie dell'*Elenco dei Prodotti a Duplice Uso* relativo alla normativa europea sulle esportazioni forniscono un'idea della potenziale vastità di tale ambito:

- Categoria 0 - Materiali nucleari, impianti e apparecchiature;

[59] Acosta, M., Coronado, D. e Marin, R. (2011), "Potential Dual-Use Of Military Technology", p. 338

- Categoria 1 - Materiali speciali e relative apparecchiature;
- Categoria 2 - Trattamento e lavorazione dei materiali;
- Categoria 3 - Materiali elettronici;
- Categoria 4 - Calcolatori;
- Categoria 5 - Telecomunicazioni e sicurezza dell'informazione;
- Categoria 6 - Sensori e laser;
- Categoria 7 - Materiale avionico e di navigazione;
- Categoria 8 - Materiale navale;
- Categoria 9 - Materiale aerospaziale e propulsione.

Tali categorie sono dettagliate nelle 400 pagine di *Allegato I* al *Regolamento 2021/821 del Parlamento europeo e del Consiglio*[60].

Tra questi, esempi di tecnologie dual-use sono tipicamente le ICTs sia hardware (es. ricevitori segnale navigazione satellitare) che software (es. criptografia). Vi rientrano sensoristica, materiali avanzati e, tradizionalmente, tecnologie e prodotti in ambito chimico, biologico, radiologico e nucleare (CBRN). Tra i servizi dual-use è possibile considerare le immagini satellitari elaborate per fornire "geospatial information" (come nel caso di e-GEOS per i dati COSMO-SkyMed o del Copernicus Emergency Management Service). Come conoscenza codificata, si riporta l'esempio di algoritmi di ottimizzazione della ricerca operativa che possono essere applicati sia al calcolo del percorso di trasporti pubblici, che per rotte di attacco in ambito militare. Ma anche tecniche di project management nate in ambito militare e passate nel settore inverso (es. Program Evaluation and Review Technique, PERT) e viceversa (es. Lean Production e del Total Quality Management, TQM). E brevetti di tecnologie di fibre e tessuti utilizzati per abbigliamento specifico dal militare al civile (es. sport) e viceversa. Tra le piattaforme dual-use vi sono elicotteri utility (multiruolo) in primis, come AW101, che nasce per la Marina Militare italiana e dal quale viene ricavata una versione per la sicurezza (polizia giapponese), e vip; l'HH139A che nasce civile; e AW139, del quale viene fatta una versione militare. Tra i sistemi dual-use vi sono la costellazione satellitare per osservazione terrestre COSMO-SkyMed, il sistema dell'UE di navigazione satellitare globale Galileo, i satelliti SICRAL della Difesa italiana, il satellite Access on THeatres and European Nations for Allied forces - French Italian Dual Use Satellite/Athena-Fidus) realizzato attraverso accordo delle rispettive Difese e agenzie spaziali nazionali, e alcuni velivoli a pilotaggio remoto (es. FALCO).

---

60 PE e Consiglio dell'UE (2021), "Regolamento (UE) 2021/821 che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso (rifusione)", 11 Giugno

La distinzione fra piattaforme e sistemi non è sempre chiara né oggettiva ma, in generale, il sistema è già integrato (es. satellite, velivolo da combattimento, carro da battaglia, nave combattente), mentre la piattaforma è integrabile (es. alcuni elicotteri, navi, mezzi terrestri che possono ricevere armamenti ed equipaggiamenti diversi). In alcuni casi di tecnologie e prodotti dual-use esiste una progettazione ab initio dual-use (es. COSMO-SkyMed), mentre in altri è intervenuto un adattamento per applicazioni nell'ambito del mercato inverso. Esempi di questo secondo caso sono le piattaforme dei satelliti SICRAL, che sono operati e gestiti in autonomia dalla Difesa e volti a soddisfare le esigenze operative strategiche e tattiche nazionali, ma con la fornitura di servizi in ambito sia NATO sia nazionale, in materia anche di sicurezza e protezione civile.

SETTORE PRIVATO

AZIENDA

La tipologia di azienda può influire nella scelta di perseguire o meno una strategia di R&S dual-use o di trasferimento di tecnologie e prodotti dual-use per trarre profitto dai diversi mercati civile/sicurezza e militare. Questa può essere, ad esempio, una PMI o una large company e trovarsi in posizioni diverse nella supply chain (da prime contractor a sub-contractor/supplier), essere partecipata dallo Stato o meno, con differenti implicazioni.

Alcuni ritengono che le grandi aziende abbiano a disposizione maggiori risorse per differenziare il business (strutture di R&S, fonti di finanziamento, competenze, facilities, etc.), ma che possano risultare più lente nel cambiamento a causa di una catena gerarchica e manageriale più lunga. In generale, infatti, le PMI sarebbero più flessibili e disponibili al cambiamento di quanto non lo siano le grandi aziende. Secondo altri, invece, una dimensione ridotta della struttura potrebbe essere un fattore limitante nello sviluppo verso il mercato inverso, cioè generalmente più l'azienda è piccola minore dovrebbe essere il livello di diversificazione che può sostenere. Altri ancora, invece, ritengono che la sostenibilità dei costi non sia necessariamente direttamente legata alla taglia dell'impresa.

Ma è soprattutto la posizione di partenza, e cioè se si tratti di un'azienda tradizionalmente operante nel mercato civile/sicurezza o militare, ad avere una valenza rispetto alla capacità di superare le barriere di accesso al mercato inverso che si combina con altri fattori caratterizzanti l'azienda stessa.

BUSINESS STRATEGY

La business strategy riguarda le strategie di cambiamento, come quelle di sviluppo e diversificazione verso mercati (clienti) e tecnologie/prodotti del mercato inverso. La decisione di prendere in considerazione il potenziale della dualità è situata a livello strategico e l'attuazione di cambiamenti comporta differenti livelli di rischio. Più l'azienda si allontana dal proprio core business iniziale verso clienti collegati o nuovi o verso tecnologie/prodotti affini o nuovi (da sviluppare) o verso entrambe le direzioni, maggiori sono i costi economico-finanziari (e di transazione) necessari per estendere, adattare o acquisire competenze valide per il mercato target.

Secondo alcuni, tali scelte possono essere facilitate da technology brokering office interni alle aziende e capaci di osservare e predire le linee di sviluppo dell'innovazione tecnologica. Ciò può avvenire anche tramite consulenze di intermediari tecnici esterni. Alcuni ritengono che in tale contesto la sostenibilità economico-finanziaria e il rischio siano proporzionali – la prima direttamente, il secondo inversamente – alla possibilità di valorizzare nel mercato inverso le stesse strutture di produzione e di costi nonchè le stesse capacità chiave espresse nel mercato di provenienza[61]. La verifica della sostenibilità dei costi economico-finanziari e di transazione della diversificazione deve essere considerata su una base di medio-lungo periodo. Tale analisi di sostenibilità è anche strettamente connessa alla conoscenza di eventuali aiuti, in particolare per le PMI, forniti da strutture statali, regionali e di categoria.

In ambito militare la logica non è commerciale, ma basata su finanziamenti pubblici anche anticipati (mentre in generale in ambito civile si ha una fatturazione con le vendite finali), e la presenza di importanti costi non ricorrenti può non permettere l'emergenza di un punto di ammortamento degli investimenti in R&S nel ciclo di vita/curva di adozione della tecnologia. Il punto di ammortamento è, inoltre, potenzialmente soggetto ad ulteriori costi inattesi, dovuti a negoziazioni di ulteriori requisiti tecnici sopravvenuti nella produzione di un sistema e ad incertezza su eventuali ritardi nella consegna del sistema. Tale situazione potrebbe spingere alla realizzazione di tecnologie/prodotti dual-use per aumentare il ritorno degli investimenti in R&S. Secondo alcuni rappresentanti istituzionali europei dovrebbe attuarsi un passaggio dalla cultura "grant" a quella "loan" per alcuni settori della difesa. La Difesa dovrebbe restare a carico della collettività, ma al suo interno bisognerebbe tracciare chiaramente una linea tra attività alle quali non si può chiedere di generare profitti, e che devono essere assunte a perdita, e altre che invece possono e devono avere una logica

[61] Mérindol, V. e Versailles, D. W. (2015), "La dualité dans la stratégie des entreprises", ECODEF, Gennaio, p.3

economica. E se è generalmente vero, tranne alcune eccezioni, che i programmi nel settore della difesa non sempre ottengono un ritorno significativo, ovvero bilanciato rispetto all'investimento fatto, questo è meno vero se si considerano gli spillover tecnologici. Le tecnologie più avanzate, infatti, sono spesso state sviluppate in ambito militare ed anche se il ritorno è stato contenuto nel settore difesa queste hanno avuto un impatto significativo in altri settori civili (es. settore spaziale, aeronautico, etc.).

Aziende operanti nel settore della difesa stanno allargando la propria attività, per determinate tecnologie e prodotti, anche al mondo civile commerciale in quanto quest'ultimo offre un numero più elevato di possibili acquirenti. Si consideri, ad esempio, che una quota rilevante e crescente dei ricavi di industrie dell'aerospazio e della difesa deriva dal mercato civile/sicurezza: 130 miliardi di euro nel 2019 (rispetto ai 97 miliardi dell'anno precedente) che rappresentano il 51.5% del fatturato annuo, con un impatto di 109 miliardi sull'export europeo (82% della produzione totale)[62]. Le stesse industrie della difesa dipendono, in parte, dal mercato civile/sicurezza: ad esempio, nel 2019 circa il 32% dei ricavi di Leonardo non è derivato da applicazioni per la difesa – un trend confermato anche da Thales (49% dei ricavi) e da Airbus (83%)[63]. Si tratta di considerare il dual-use non sotto la sola prospettiva di una categorizzazione o dispositivo pubblico volto a favorire sinergie civili/sicurezza – militari e l'inserimento delle PMI nelle filiere produttive, ma come dimensione chiave della strategia delle grandi imprese militari per preservare la competitività in un contesto di crescenti attività in ambito civile. Strategia sulla dualità che varia a seconda delle caratteristiche specifiche dell'azienda.

Con la premessa che generalmente in ambito civile prevalgono costi ricorrenti e in ambito militare non ricorrenti, è possibile osservare che uno degli argomenti a favore di sviluppo e diffusione di tecnologie e prodotti dual-use risiede, infatti, nella possibilità di sfruttare economie di scala. Ad esempio, nel caso di prodotti Commercial Off-the-Shelf (COTS), Non-Developmental Item (NDI) o di tecnologie e prodotti che richiedano limitati adattamenti nel trasferimento da un settore all'altro, esiste la possibilità di diversificare ed espandere la propria quota di mercato sfruttando appunto economie di scala non solo nelle attività di R&S, ma in ogni fase del processo innovativo inclusa la produzione. Ovviamente anche in ambito militare molto dipende dalla tecnologia o prodotto specifici: un sistema elettronico di protezione delle frontiere o di sorveglianza del traffico marittimo richiede investimenti governativi e decisioni politiche in virtù della sua importanza, costo, durata nel

---

62 AeroSpace and Defence Industries Association of Europe (ASD), "2019, Facts & Figures"; CE, "EU Aeronautics Industry"

63 ASD, "2019, Facts & Figures"

tempo, tali da poter essere acquisito in pochissimi esemplari; di converso, i singoli apparati/sensori che lo compongono possono avere altre applicazioni e beneficiare di economie di scala.

Alcuni individuano settori ad alto potenziale dual-use, in cui è concepibile un ri-orientamento della struttura aziendale verso tecnologie e prodotti del mercato inverso nei seguenti: cyber-security/defence e ICTs, smart materials, sistemi veicolari o robotici a guida/pilotaggio remoto, sistemi per sorveglianza del territorio e/o contrasto a minacce esplosive/chimico–batteriologiche, sistemi aerospaziali e relative fonti energetico-propulsive. Nella scelta sul ri-orientamento è da rilevare che la capacità tecnologica non è equivalente alla validità economica. Infatti va verificata la sostenibilità del rapporto tra esigenze operative da soddisfare in ambito ad esempio civile/sicurezza e costi della soluzione in ambito inverso, ad esempio militare. I casi del Boeing 767/KC-46 e dell'A400M sarebbero indicativi. Nel primo caso, l'adattamento di un velivolo di linea già esistente verso il Boeing KC-46 Pegasus (aereo militare per il rifornimento in volo e trasporto strategico) si è dimostrato più lungo e complesso del previsto; nell'altro, lo sviluppo e la costruzione di un prodotto militare ex novo da parte di un costruttore tradizionalmente civile (Airbus) si è tradotto in ripetuti ritardi e costi extra.

COMPETENZE E CULTURA

La posizione di partenza in termini di core business strategico/tradizionale ha un peso fondamentale. Più l'azienda si allontana dal proprio core business iniziale, maggiori sono i costi non solo economico-finanziari, ma di transazione (es. risorse capacitive e di tempo per la comprensione di quadri istituzionali e regolamentari del mercato inverso) necessari per estendere, adattare o acquisire competenze valide per il mercato target.

La posizione di partenza ha una forte valenza anche di tipo culturale e il fattore culturale è centrale: come già riconosciuto da anni da diversi autori, ad esempio, incide fortemente sulla realizzazione di spin-off. Un'impresa che pensa ad una tecnologia per un privato cittadino e una che lavora per la Difesa divergono in modo quasi filosofico. Per sfruttare la potenzialità del dual-use, in alcuni casi bisogna essere aperti alle dinamiche del mercato civile/sicurezza, in altri comprendere e gestire specificità del mercato della difesa. Questo è rilevato anche in contesti diversi da quelli euroatlantici, in cui le difficoltà collegate alla conversione sono associate principalmente a cultura aziendale e approccio del management, piuttosto che a questioni tecnologiche e ingegneristiche[64].

---

64 Li, X. e Lei, Y. (2007), "Research on Dual-Use Technology and Dual-Use Policies in National Innovation System", p. 207

Il passaggio al mercato inverso richiede un cambio culturale importante di apertura all'innovazione dal, e verso il, mercato inverso. Un'eccessiva rigidità culturale nei comportamenti produttivi e commerciali, che non vengano adattati al mercato inverso, può determinare per un'azienda il fallimento della diversificazione. L'elemento culturale sembra assolutamente trasversale dal momento che è spesso associato ad altri fattori che influenzano la scelta di un'azienda di perseguire una strategia di R&S dual-use o di trasferimento di tecnologie e prodotti dual-use. Ad esempio, molti esperti e stakeholder rilevano che l'organizzazione della funzione R&S influisce, ma deve essere accompagnata da mentalità e cultura appropriate che solo parzialmente possono essere determinate dal tipo di organizzazione; e ancora, sui processi di sviluppo e/o trasferimento di tecnologie/prodotti dual-use, si osserva che se tali processi sono strutturati e documentati favoriscono il successo delle iniziative, ma resta essenziale che sia creata la cultura professionale adeguata.

Il fattore culturale riguarda anche gli shareholder che influiscono con le loro aspettative e con il loro livello di disponibilità al cambiamento e all'investimento sulle scelte strategiche dell'impresa. La diversificazione comporta l'assunzione di rischi aziendali di cui gli shareholder e gli stakeholder devono essere a conoscenza. Nelle aziende ci possono essere casi in cui attività di foresight sono concepite come strettamente legate alla funzione R&S (peso più strutturale), altri in cui risiedono in livelli manageriali di alto livello (peso più culturale)[65]. Secondo diversi rappresentanti dell'industria, ma anche di istituzioni UE, il grande peso della cultura di impresa (e delle Divisioni) è costantemente sottovalutato nelle analisi. Più in generale, il fattore culturale è così determinante da poter restare assolutamente impermeabile a schemi teorici volti a far sì – semplificando – che un prodotto civile/sicurezza diventi militare o viceversa.

CONOSCENZA E COMPLIANCE

Ultimo, ma non ultimo, lo sviluppo e la diffusione di tecnologie e prodotti dual-use sono influenzati dalla conoscenza e compliance aziendale verso il quadro istituzionale e di regolamentazione del mercato inverso e del mercato dual-use nazionale, europeo e internazionale.

Nel caso dell'export dual-use, soprattutto militare, conoscenza e compliance sono una condizione per evitare il rischio di non essere autorizzati ad esportare, di incorrere in penali contrattuali a causa di ritardi nelle consegne, di subire potenziali sequestri da parte delle

---

65 Battistella, C. (2014), "The organization of Corporate Foresight: a multiple case study in telecommunication industry", Technological Forecasting and Social Change, p. 68

autorità doganali o, ancora, di subire sanzioni dopo aver effettuato le esportazioni. Alcuni esperti ritengono che l'impatto del Regolamento export dual-use e delle conseguenze in capo all'azienda dovrebbe iniziare ad essere valutato già in fase di procurement per le aziende commerciali o di ingegneria per le quelle industriali. Le difficoltà possono essere aggravate da uno scarso controllo della supply chain da parte dell'industria, che tende a schiacciare nel momento della vendita/esportazione gli oneri dettati dalla normativa, subendo conseguenze negative in termini di efficienza e competitività. L'export control è un tema che dovrebbe invece interessare trasversalmente tutta l'attività d'impresa coinvolgendo aspetti di compliance che impattano su processi di carattere manageriale e gestionale e non solo tecnico ed operativo[66]. In particolare non sembra sufficiente che il livello di consapevolezza sia elevato solamente nei settori maggiormente coinvolti, come l'import/export o il legal; ma anche altri settori aziendali, che apparentemente sembrerebbero poco coinvolti, dovrebbero essere in possesso di un livello base di preparazione. A titolo esemplificativo, il reparto amministrativo potrebbe imbattersi in un pagamento attraverso un intermediario finanziario "listato", o ancor di più, un ufficio vendite dovrebbe essere adeguatamente istruito onde evitare di incorrere, magari attraverso un'operazione triangolare, nella conclusione di un contratto in cui, a differenza delle apparenze, l'end-user si riveli essere diverso dall'acquirente. I programmi di conformità interni, generalmente, devono considerare anche norme extraterritoriali e devono rispondere agli standard stabiliti dalle autorità di controllo corrispondenti, che potrebbero includere processi a prova di errore ("mistake-proofing processes"), intensa formazione e strutture di controllo e, di conseguenza, investimenti rilevanti per l'azienda, che sono tuttavia giustificati al fine di evitare possibili sanzioni e negativa reputazione. Secondo alcuni, un approccio tradizionale alla gestione compliant della supply chain potrebbe, inoltre, non essere sufficiente. Per gestire i processi legati alle limitazioni normative in ambito export dual-use, alcuni hanno infatti sviluppato piattaforme innovative, frutto del know-how normativo e di soluzioni informatiche ad hoc a supporto dei principali attori aziendali coinvolti, attraverso cui è possibile monitorare le varie fasi dei processi aziendali in maniera conforme, fornendo informazioni utili per gli scopi decisionali e supporto a livello operativo. Infine, la compliance verso tale regime non dovrebbe essere vista solo come un obbligo burocratico ma, se rispettata, come un enabler della competitività per l'azienda.

Possono, inoltre, rientrare nell'area di conoscenza e compliance aziendale policies e normative su standard, certificazioni, Intellectual Property Rights (IPRs) del mercato

---

66 Intervento (2016) durante il Workshop "L'export control nei settori dell'aerospazio e della difesa: compliance, sicurezza e competitività", Centro Studi Geopolitica.info, Roma, 17 marzo

inverso/dual-use nel cui quadro si inseriscono accordi contrattuali. A seconda dei casi, tale conoscenza favorisce il dual-use o ne è condizione di realizzazione, come nel caso di standard e certificazioni obbligatorie.

La presenza di standard nel mercato target inverso può facilitare l'ingresso in tale mercato, rendendo certa la qualità, la trasferibilità e l'interoperabilità di tecnologie e prodotti e funzionando da facilitatore per progetti di collaborazione in R&S[67]. Infatti la dualità è direttamente proporzionale alla compatibilità di standard tra ambiti civile/sicurezza e militare. Tale conoscenza risulterebbe più onerosa per le PMI, generalmente dotate di risorse più limitate. Così come pure l'opportunità per l'azienda o per un'organizzazione pubblica di partecipare alla definizione di standard varia da caso a caso, ma sempre implica costi economici e di transazione (es. costi amministrativi, per attività di lobbying, e in termini di tempo) più gravosi per la PMI.

I diritti della proprietà intellettuale sono fondamentali anche per R&S dual-use e trasferimento di tecnologie e prodotti dual-use per il controllo di tecnologia e prodotti brevettati nell'interazione tra settore civile/sicurezza e militare[68]. Specialmente in ambito internazionale, la mancanza di chiarezza nei requisiti relativi a diritti della proprietà intellettuale può portare le imprese a credere che vi sia una protezione sufficiente dei propri IPRs, quando invece manca, oppure ad astenersi dal fare investimenti in determinate iniziative o in determinati Paesi per timore di non essere sufficientemente garantiti. Gli IPRs possono rappresentare dunque un ulteriore appesantimento del quadro normativo a discapito soprattutto di PMI che hanno risorse più limitate per la comprensione e la protezione dei propri IPRs. Ma anche realtà aziendali più grandi, nonostante indagini lunghe e costose, non sempre riescono ad ottenere certezza della protezione degli IPRs, specialmente in alcuni Paesi.

Possono, infine, rientrare nell'area di conoscenza e compliance aziendale la capacità di accesso ad informazioni e la capacità di application relative ad opportunità di R&S e procurement del mercato inverso o dual-use. Tale conoscenza sembra essere più complessa da parte di PMI, dotate di minori mezzi per accedere a consulenze e studi. Aziende che abbiano i mezzi possono essere facilitate dall'assunzione di un officer specializzato esterno (nella formulazione dei progetti/proposte/offerte) o dalla formazione di uno interno.

---

67 EDA (2014), "Your Guide to European Structural Funds for Dual-use technology projects", p.1

68 Mérindol, V. e Versailles, D. W. (2010), "Dual-use as Knowledge-Oriented Policy: France during the 1990–2000s", International Journal of Technology Management, p. 82

Il quadro della conoscenza e compliance è infine complicato dalla crescente presenza di transnational companies, con unità che hanno sede od operano, e quindi devono rispettare, diversi sistemi nazionali normativi e di regolamentazione.

CIV/SIC → MIL

È un passaggio che appare molto più complesso rispetto all'inverso.

AZIENDA

Alcuni osservano che grazie all'aumento di outsourcing nella defence supply chain, il ruolo delle PMI sia cresciuto. Anche lo European Defence Action Plan (EDAP) della CE, facendo riferimento al possibile utilizzo del pre-commercial procurement in ambito difesa, incoraggiava la partecipazione tra gli altri di PMI operanti nella innovazione dual-use[69]. La maggior parte degli esperti, però, concorda sul fatto che le PMI siano svantaggiate nella diversificazione verso il mercato della difesa che è soggetto a maggiori vincoli rispetto a quello civile/sicurezza. Per le PMI sarebbe opportuno o necessario agire tramite una prime large company (tipicamente a partecipazione statale) già consolidata nel settore e introdotta a livello nazionale, in organizzazioni come NATO ed EDA e in accordi bi- o multilaterali. Altri ritengono che, una volta entrata nel mercato della difesa, una PMI abbia, però, generalmente agilità e competitività maggiori rispetto ad una large company e che possa risultare più versatile rispetto a PMI esclusivamente militari.

BUSINESS STRATEGY

Alcuni ritengono che le PMI tradizionalmente operanti nel settore civile, ad eccezione di casi specifici, non abbiano sufficiente conoscenza di tecnologie e prodotti militari ed entrature nel mercato della difesa per favorire R&S dual-use e/o trasferimento di tecnologie e prodotti. Migliore il caso in cui, ad esempio, per soddisfare esigenze di interoperabilità una PMI possa far leva su proprie tecnologie di sicurezza. Si rileva, inoltre, che le PMI coinvolte nel mercato della difesa sono quasi esclusivamente coinvolte in attività dual-use[70]. Una large company operante in ambito civile/sicurezza potrebbe fare leva su una ampia customer base, per diversificare il proprio business verso il settore della difesa, nel caso in cui tecnologie e prodotti sviluppati in-house, di cui sia proprietaria, siano adattabili a requisiti del cliente militare.

---

69 CE (2016), "Towards a more competitive and efficient defence and security sector", p. 8

70 Europe Economics (2014), "Enhancing support to SMEs", p.130

Alcuni ritengono che ciò sia possibile per alcune tecnologie, particolarmente del tipo ICTs. Tecnologie di base possono derivare dal settore militare, ma sempre di più dal settore civile, come infatti l'ampio campo dell'elettronica e dell'informatica. Dal punto di vista economico risulterebbe più complesso il passaggio da civile/sicurezza a militare. Lo sviluppo o l'adattamento di prodotti che possano riscuotere l'interesse militare, ma nati per il mercato inverso, può avere un costo elevato legato alla ri-progettazione. Costo che secondo alcuni potrebbe essere mitigato da alcune misure che potrebbero essere adottate lato militare anche con la consulenza e il supporto dei Centri di Test and Evaluation (T&E) della Difesa. Ad esempio, i costi di test/omologazione potrebbero essere compensati dal prezzo riconosciuto alla tecnologia o alla conoscenza ed il rischio finanziario, per le PMI o le università, potrebbe essere contenuto da meccanismi di sostegno delle prove sino a livello di dimostratore tecnologico (Technology Readiness Level, TRL 4-6).

Qualora invece la diversificazione sia una decisione autonoma dell'azienda, i costi di transazione devono essere sostenuti da un business case che consenta ritorni sufficienti a giustificare l'investimento. A tal fine, è indispensabile che la funzione aziendale R&S si interfacci costantemente con esperti e analisti del settore difesa, meglio se inseriti in alleanze o organizzazioni internazionali, al fine di definire il livello di vantaggio economico o tattico prevedibile nel medio-lungo periodo. Secondo alcuni commentatori, dal punto di vista del cliente militare lo sviluppo di una tecnologia è fortemente condizionata dall'esigenza (market push), mentre non appare realmente interessante un'organizzazione che si costituisca come technology push.

Secondo alcuni esperti, modelli di open innovation sarebbero più facili da realizzare in ambito militare perché il confronto con gli end-user sarebbe agevolato dall'identificazione chiara ed univoca di questi ultimi e dal loro numero limitato. Inoltre, le esigenze operative e funzioni richieste in tale ambito cambierebbero più lentamente nel tempo. Secondo altri, invece, l'open innovation sarebbe maggiormente legata al settore civile/sicurezza perché spesso le aziende innovative non sarebbero interessate ai requisiti degli end-user militari o non sarebbero in grado di comprenderli. Per l'innovazione militare l'approccio resta di tipo top-down e parte dall'end-user. La condivisione e verifica dei requisiti eventualmente comuni all'ambito civile/sicurezza parte dunque maggiormente dagli end-user militari ed arriva al fornitore, anche per quanto riguarda i bricks tecnologici.

In ambito difesa, è stato osservato che nel caso di sviluppo di sistemi per il mercato militare che integrino COTS, la possibilità di poter disporre di questi ultimi potrebbe accelerare le tempistiche di sviluppo. Si pensi, ad esempio, all'adozione di software open source per applicazioni militari. Questa è un'ipotesi crescente considerando che oggi il trend

sembra invertito ed è l'innovazione civile a nutrire quella militare (come nel caso di alcune ICTs civili che non necessitano di particolari modifiche per essere inserite in sistemi militari). Questo è possibile anche grazie ai progressi fatti sui componenti COTS, tali da poterli, in alcuni casi, paragonare a quelli embedded in termini di performance. D'altra parte, è opportuno tener conto di eventuali ulteriori costi di sviluppo legati ai COTS, sia nel caso di eventuali adattamenti per l'applicabilità a sistemi con requisiti molto diversi da quelli già commercialmente applicabili e non sempre correttamene previsti, sia per la pianificazione di più frequenti aggiornamenti di prodotti COTS (in particolar modo Information Technology, IT), a causa di una obsolescenza, con un rateo molto elevato rispetto ai prodotti militari.

COMPETENZE E CULTURA

Aziende tradizionalmente operanti in ambito civile/sicurezza che vogliano entrare nel mercato militare sono poste in una posizione di svantaggio per maggiori costi di transazione dovuti ad investimento di tempo e di risorse (finanziarie e capacitive) nella comprensione delle regole del mercato inverso. Il problema dell'accesso delle aziende civili (o in generale nuove) al mercato della difesa è infatti tipicamente connesso alla difficoltà di comprensione delle sue peculiarità, più che ad una questione tecnologica. Un'impresa abituata a vendere tecnologie e prodotti civili/sicurezza a privati cittadini, pure avendo tecnologie/prodotti vendibili in ambito militare, dovrà apprendere procedure d'appalto della Difesa, rispettare condizioni di Security of Supply e di Security of Information, etc.

CONOSCENZA E COMPLIANCE

Lo sviluppo e la diffusione di tecnologie e prodotti dual-use sono influenzati dalla conoscenza e compliance aziendale verso il quadro istituzionale e di regolamentazione del mercato inverso militare e del mercato dual-use nazionale/europeo/internazionale.

La conoscenza e compliance aziendale verso normative export mercato dual-use e militare UE e nazionali sono condizioni per poter operare in determinati mercati, e tale conoscenza risulta largamente più complessa per imprese che non sono del settore. Questo è particolarmente vero anche per la conoscenza delle procedure di procurement. Quanto al regime UE di esportazione dual-use verso Paesi extra-europei (ed in misura minore intra-europei), le diverse trasposizioni ai livelli nazionali comportano complessità da gestire che possono rendere necessario per un'azienda avvalersi di export compliance officer interni o outsourced. Il dual-use potrebbe rappresentare, infatti, un ostacolo all'esportazione, un rischio non sempre preventivabile dal momento che la consapevolezza circa la natura dual-

use dei beni arriva spesso solo in una fase successiva alla produzione, grazie ad input di consulenti esterni all'impresa in fase di esportazione (spedizionieri, trasportatori, agenti doganali, avvocati, etc.). Dal punto di vista aziendale, questi aspetti di regolamentazione possono giungere a pesare in maniera importante su aspetti amministrativi della distribuzione e della logistica e appunto dell'export, più che sul ciclo produttivo in sé[71].

Standard e certificazioni obbligatori sono condizione per operare nel mercato target e possono costituire barriere all'ingresso nel mercato nel caso in cui l'azienda non abbia appropriate risorse per affrontare costi economici e di transazione relativi alla conoscenza e compliance con standard stringenti, come nel caso del mercato della difesa (es. resistenza di materiali a determinate condizioni). Le aziende già operanti in ambito difesa sono in una posizione di vantaggio nel breve periodo rispetto a quelle non già operanti nel settore e che devono modificare i propri processi per implementare standard obbligatori. Come per gli standard, anche la compliance aziendale verso le certificazioni sconta la difficoltà legata alla scarsa armonizzazione delle policies nazionali e include per le aziende il rischio di costi aggiuntivi per la richiesta di certificazioni diverse nei vari Paesi per la stessa tecnologia, prodotto, processo. Come rilevato da alcuni autori, l'armonizzazione delle politiche di standardizzazione e certificazione potrebbe favorire in maniera importante le PMI interessate ad operare nel settore della difesa oltre i confini nazionali[72].

Le barriere al trasferimento di tecnologia legate ai regimi IPRs possono essere di diverso tipo. Per un'azienda tradizionalmente operante nel settore civile/sicurezza potrebbero intervenire dei meccanismi disincentivanti rispetto alla partecipazione in progetti di R&S in ambito difesa e quindi rispetto all'ingresso nel mercato inverso, a causa della possibile modifica dei regimi di attribuzione, accesso, uso (Ownership, Access, Use) degli IPRs a seguito della partecipazione a tali progetti (es. appropriazione degli IPRs da parte di un membro del consorzio o da parte del finanziatore della R&S), ma anche a seguito di obblighi di riservatezza sopraggiunti e dunque impossibilità di riutilizzo in ambito civile di tecnologie e prodotti sviluppati in ambito difesa.

Anche per la capacità di accesso ad informazioni e capacità di application relative ad opportunità di R&S e procurement del mercato militare o dual-use, aziende provenienti dal mercato civile/sicurezza incontrano maggiori difficoltà. La complessità di comprensione delle procedure e i costi, anche di transazione (ad esempio anche per barriere linguistiche per bandi nazionali) hanno un impatto soprattutto sull'abilità di PMI di competere rispetto a

---

71 Foti, P. (2012), "I sistemi dual-use: sviluppo, applicazioni e tecnologie abilitanti", Project Work del Master Universitario di II livello Homeland Security, Sistemi, Metodi e Strumenti per la Security e il Crisis Management, p. 21

72 Europe Economics (2014), "Enhancing support to SMEs", p. 83

grandi imprese che si presume abbiano risorse e capacità superiori per affrontare tali aspetti.

MIL → CIV/SIC

Teoricamente più agevole sembra il passaggio da militare a civile/sicurezza (dual-use) - almeno dal punto di vista tecnologico - anche se alcune opinioni sollevano possibili criticità anche in tali casi.

AZIENDA

Secondo alcuni, le PMI tradizionalmente operanti nel settore della difesa avrebbero un bagaglio tecnologico focalizzato su alcuni business specifici e sarebbero svantaggiate nella diversificazione perché, lavorando solo con interlocutori militari, avrebbero un'esperienza limitata ad un contesto particolare, ben diverso dal mercato civile/sicurezza. Le large companies sarebbero facilitate rispetto alle PMI a transitare dal settore difesa a quello dual-use perché possiederebbero una gamma di prodotti più vasta, nella quale individuarne di adattabili al mercato inverso e perché possiederebbero maggiori risorse per farlo. Secondo altri, le large companies sarebbero meglio strutturate per affrontare i processi di diversificazione, ma più vincolate ai prodotti della loro filiera/catena o gruppo. Vanno comunque considerati eventuali limiti dovuti ad accordi di esclusiva, con le autorità pubbliche della Difesa, per determinati prodotti militari con impegno a non adattarli per il mercato inverso.

BUSINESS STRATEGY

Secondo alcuni, il know-how militare fornirebbe un valore aggiunto maggiore per l'inversione a dual-use per aziende originariamente operanti nel settore della difesa che concepiscano il potenziale dual-use come componente di una strategia di diversificazione. Alcuni ritengono che per una PMI sia ipotizzabile una preferenza per le modalità di trasferimento esterno (diretto o con adattamento): ne è esempio una società spin-off, creata ad hoc e comunque controllata, soluzione che terrebbe i modelli organizzativi dell'azienda completamente separati e, di conseguenza, non recherebbe problemi per riaccreditare i processi interni secondo i vari standard di classifica e di security.

Secondo altri, essendo in linea generale le fonti di finanziamento da parte dei clienti per attività di R&S focalizzate su sviluppo di prodotti specifici per uso militare, vi è un numero limitato di attività R&T, in genere a livello TRL 2-3, effettuate in aree che potrebbero avere un uso dual-use. Si tratta principalmente di attività di ricerca sui materiali e su tecnologie

legate alla sensoristica, al software e all'elettronica. Va precisato che tali attività di R&T, sia finanziate dal cliente che autofinanziate, sono prevalentemente indirizzate a finalità militari e che i risultati che possono emergere per applicazioni dual-use sono principalmente non conseguenti ad una finalità primaria di sviluppare tecnologie dual-use, ma un risultato secondario. Inoltre, una volta che la maturità tecnologica aumenta oltre il livello TRL 2-3, i risultati diventano più specificatamente ad uso militare, mentre secondo altri anche tecnologie per applicazioni militari a TRL 3-6, possono trovare forti punti in comune con quelle del settore civile/sicurezza.

COMPETENZE E CULTURA

Per sfruttare la potenzialità del dual-use bisogna essere aperti alle dinamiche del mercato civile/sicurezza. Anche per le large companies, considerate avvantaggiate nella diversificazione verso il mercato civile/sicurezza alcuni osservano che, a meno che la strategia della large company non sia fortemente orientata al dual-use, la maggior rigidità dei processi interni e della cultura aziendale comportino effetti negativi per la realizzazione della diversificazione.

CONOSCENZA E COMPLIANCE

In un'azienda che si colloca nel settore militare, oltre alla conoscenza della normativa legata all'esportazione di materiale cosiddetto di armamento, anche la conoscenza della normativa che regola le movimentazioni di beni dual-use dovrebbe essere conosciuta. Questa osservazione, che sembrerebbe scontata, secondo l'esperienza diretta di alcuni esperti del settore legale non lo è.

In ambito civile, l'ampio riconoscimento di standard della categoria International Organization for Standardization (ISO) fa sì che non vi siano differenze significative a livello di politiche di standardizzazione nazionali, anche in virtù della logica prevalentemente market-oriented del settore: non vi sono, al contrario di quanto avviene nella standardizzazione militare "top-down", differenze significative tra i singoli Paesi derivanti dalla diversa struttura dell'apparato militare. In ambito sicurezza esistono a livello UE iniziative della CE per la creazione di standard basati sulla volontaria cooperazione tra vari stakeholder, incluse industrie e autorità pubbliche.

Le barriere al trasferimento tecnologico legate ai regimi IPRs possono essere di diverso tipo. Ad esempio, aziende tradizionalmente operanti nel campo della difesa che vogliano diversificare verso il mercato civile/sicurezza con una tecnologia precedentemente sviluppata in un progetto di R&S di difesa, potrebbero incorrere in restrizioni derivanti dalle

condizioni degli IPRs stabilite nel contratto tali da non permettere il trasferimento. In alcuni casi, infatti, il trasferimento potrebbe dover essere soggetto al controllo governativo, per la rilevanza strategica nazionale che assumono le tecnologie di impiego militare. Al contrario, aziende che operino tradizionalmente nel settore della difesa e non avessero significativi obblighi su IPRs, sarebbero avvantaggiate nello sfruttamento commerciale in ambito non-difesa.

ORGANIZZAZIONE R&S E TRASFERIMENTI TECNOLOGICI

OPEN INNOVATION

L'organizzazione della funzione R&S può essere di tipo technology push (inside-out innovation) o market push (outside-in innovation). In entrambi i casi, si tratta di modelli lineari di innovazione con sequenza di fasi in base al TRL. Altra possibilità sono modelli di innovazione non lineari di open innovation, che combinano "technology push" (inside-out innovation) e "market push" (outside-in innovation) in tutte le diverse fasi del processo di innovazione[73]. Questo è possibile sia con approccio outside-in, sfruttando idee e tecnologie esterne per ridurre costi e tempo spesi in ricerca, sia con approccio inside-out, rendendo le innovazioni (inutilizzate) più accessibili agli utenti esterni.

Alcuni descrivono modelli di open innovation che cercano il potenziale della dualità nella relazione iterativa fra tre elementi: (1) funzioni da soddisfare caratterizzanti end-user civili/sicurezza o militari, attuali/emergenti; (2) bricks tecnologici (componenti tecnologiche di base/technological building blocks) disponibili/emergenti; e (3) tecnologie e prodotti disponibili/emergenti[74].

Bricks e tecnologie possono essere presenti anche fuori dall'ecosistema di riferimento (civile/sicurezza o militare) della funzione o comuni alle funzioni caratterizzanti end-user civili/sicurezza e militari. Tali modelli devono poter includere, nella ricerca di sinergie civili/sicurezza-militare, qualsiasi livello TRL. In tale visione, è fondamentale un confronto con gli end-user del mercato inverso fin dalle prime fasi del processo di innovazione favorendo, anche, eventuali adattamenti della tecnologia. A tale proposito, diversi practitioner si esprimono in favore di una cooperazione diretta industria-cliente pubblico (es. Pre-Commercial Procurement).

Oltre al confronto con gli end-user, vi deve essere quello con attori della R&S degli ecosistemi dei settori inversi, cercando di contrastare effetti silo interni alle imprese, alle

---

73 Schilling, M. A. e Izzo, F. (2013), "Gestione dell'innovazione", McGraw-Hill Education, p. 37

74 Mérindol, V. e Versailles, D. W. (2014), "La dualité dans les entreprises de Défense", p. 17

organizzazioni pubbliche e alle tradizionali dinamiche di scambio tra gli ecosistemi civili/sicurezza e militari. Resta che l'open innovation si basa principalmente su fenomeni di rete e richiede notevoli capacità di scouting aziendale al fine di percepire le esigenze di mercato, individuare gli interlocutori che possano introdurre tecnologie o conoscenze avanzate dal mercato inverso – e verso il mercato inverso – e produrre una risposta adeguata in tempi brevi.

BRICKS TECNOLOGICI

Ai bricks tecnologici viene attribuita potenzialità dual-use nel caso in cui possano essere comuni (o adattabili) ad esigenze operative e relative funzioni caratterizzanti end-user civili/sicurezza e militari, e quindi rappresentare un caso di sviluppo o soprattutto trasferimento di tecnologie e prodotti dual-use, sia in modelli di open innovation che indipendentemente da questi.

La questione della varietà di definizione di bricks resta aperta a varie possibilità che spaziano da COTS a sottosistemi funzionali definiti, da tecnologie solo emergenti o anche disponibili. Tutte opzioni valide ed impiegabili. Secondo alcuni, un brick semplice/componente sarebbe strutturato per un'azione autonoma e diretta e non funzionerebbe se estratto dal sistema, mentre un brick evoluto sarebbe un sottosistema connesso ad altri per espletare la propria funzione. La caratteristica semplice/evoluto sembra restare relativa, infatti ad esempio i sensori possono rappresentare brick anche complessi strutturalmente, ma sono bricks semplici in un sottosistema "evoluto" di identificazione bersagli, che è a sua volta brick in un sistema di combattimento. Sarebbe dunque il concetto di uso finale a determinare le gerarchie, ad esempio, un sistema di puntamento può operare autonomamente in una piattaforma fissa terrestre, mentre diventa sottosistema in un mezzo da combattimento mobile, terrestre navale o aeronautico.

I bricks possono essere reperibili presso un unico o più fornitori al TRL desiderato. L'individuazione di bricks, disponibili o in via di sviluppo, favorirebbe l'identificazione di R&S dual-use e/o trasferimento di tecnologie e prodotti dual-use in particolare in architetture di sistema aperte che permettono plug-in, e modulari[75]. In ambiente militare e con gruppi di studio EDA e privati questo significa che la funzionalità, non è legata ad una specifica marca o costruttore/produttore di brick (sottosistema), ma all'architettura di progetto del sistema. I bricks possono essere acquistati da/sostituiti con un corrispondente brick proveniente da

[75] Nones, M. (2019), "L'innovazione tecnologica nei settori civile e militare: oltre il dual use", Affari Esteri, a. 51, n. 187, p.153

costruttori anche di ambito civile/sicurezza che abbiano adottato gli stessi standard di architettura.

COTS/NDI

COTS/NDI costituiscono una possibile interpretazione di brick tecnologici e rappresentano per l'azienda un'alternativa a prodotti e componenti sviluppati internamente. Quanto alla potenzialità di prodotti e componenti COTS/NDI nei processi di R&S dual-use e/o trasferimento di tecnologie e prodotti dual-use, la rilevanza è concentrata sui COTS che possono essere trasferiti anche tramite inserimento in prodotti destinati al settore militare. La valutazione resta comunque strettamente legata alla tipologia/specializzazione di tecnologie/prodotti.

Alcuni esperti militari esprimono opinioni più caute sui COTS a causa di una obsolescenza più rapida rispetto al passato che necessita di una previsione sull'intero ciclo di vita, con valutazione dei costi derivanti dagli aggiornamenti, considerando che l'entità dell'adattamento può risultare di non facile definizione. I COTS sono solitamente Make, non Buy. Make implica un controllo diretto sull'attività, approvvigionamenti e qualità del prodotto. L'opzione Buy per l'acquirente comporta minori costi fissi e quindi minore capitale immobilizzato, ma essendo il COTS, in tal caso,

non in controllo diretto, è importante che il fornitore a cui ci si affida sia in grado di gestire l'intero processo, anche attraverso assistenza ingegneristica e trasferimento di conoscenze all'acquirente.

TRL

Quando si parla di R&S, va rilevato che può risultare difficile applicare una netta distinzione tra i vari livelli di maturità tecnologica e che i processi di innovazione tecnologica tendono a svolgersi meno in fasi sequenziali, rispetto a fasi parallele. Anche a causa della mancanza di dati empirici sul livello di cross-fertilisation della R&S tra i settori civile/sicurezza e militare[76], le opinioni sull'impatto del TRL su R&S dual-use e trasferimento di tecnologie e prodotti dual-use restano di diversa interpretazione. Secondo il mainstream, i livelli più bassi di TRL favorirebbero maggiormente la dualità di tecnologie e prodotti perché si collocherebbero in una fase precedente rispetto all'intervento di specifiche tipizzanti i diversi usi civili/sicurezza o militari. A livelli alti di TRL o di integrazione, la dualità richiederebbe (maggiore) adattamento per favorire un trasferimento valido.

[76] Fiott, D. (2014), "Defence R&D in Europe", European Union Institute for Security Studies (EUISS) Yearbook of European Security, p. 115

Può intervenire anche una certa differenza di interpretazione tra dualità di tecnologia (maggiormente focalizzata su caratteristiche intrinseche della tecnologia) e dualità di applicazione (focalizzata sull'uso). Nella prospettiva legata all'applicazione nei diversi livelli – sistemi, sottosistemi (che dipendono dai sistemi senza i quali non possono funzionare autonomamente), sistemi integrati e piattaforme – più si va verso la parte alta del livello di integrazione della tecnologia e più si evidenzia lo scopo dedicato ad ambito civile/sicurezza o militare. Ad esempio, se si considera il carro da battaglia, è evidente che non ci sono implicazioni dual-use, ma se si scende ai sottosistemi ve ne possono essere: sensoristica, sistema di guida, sistema di controllo trazione o propulsione.

È per questo che diversi stakeholder, basandosi su un'interpretazione focalizzata sulle applicazioni, considerano l'esistenza di piattaforme e sistemi dual-use nel senso di piattaforme e sistemi strutturate in maniera che, con limitati adattamenti, possano essere impiegati in ambito inverso[77]. Tipicamente sistemi spaziali, come Copernicus e Galileo – pilastri del programma spaziale dell'UE – sono considerati, infatti, sistemi dual-use. Ad esempio, un'immagine satellitare può fornire servizi di geo-intelligence (GEOINT) per applicazioni militari, oppure offrire servizi per l'agricoltura, lo studio del cambiamento climatico e la mitigazione di rischi e danni in caso di emergenza e disastro naturale. Allo stesso modo, la costellazione Galileo fornisce segnali di posizionamento e navigazione tramite il servizio Open Service (OS) accessibile a tutti gli utenti che lo ricevono, ma può essere utilizzata anche per il Public Regulated Service (PRS) per fornire segnali resistenti, autenticati e sicuri per FFAA e corpi di sicurezza.

Come visto, modelli di open innovation non dovrebbero essere intesi come limitati alle prime fasi TRL o, per il contesto militare, ai livelli R&T, ma dovrebbero poter comprendere l'intero processo di innovazione, inclusi livelli elevati di TRL. Infatti la dualità, la ricerca di sinergie tra gli ambiti civile/sicurezza e militare, sia a livello di R&S dual-use che di trasferimento di tecnologie e prodotti dual-use, è, secondo altri stakeholder, potenzialmente possibile in ogni livello di maturità tecnologica, dal momento che non esiste uno specifico livello di TRL in cui la possibilità di R&S di tecnologie e prodotti dual-use finisce e lo sviluppo di tecnologie e prodotti specificatamente civili/sicurezza o militari inizia: ogni settore, ogni tecnologia e prodotto ha proprie peculiari caratteristiche e condizioni[78].

---

[77] Gen. Rosso, A. (2014), intervento durante la Conferenza "Gli elicotteri duali nel campo della sicurezza e difesa", IAI con il sostegno di Agusta Westland, Roma, 28 Ottobre

[78] Intervento (2014) durante il Workshop "Accelerating Dual-Use potential of Key Enabling Technologies", Working Group on Dual Use KETs, DG Enterprise and Industry, CE, Bruxelles, 28 Novembre

R&S DUAL-USE E TRASFERIMENTI DI TECNOLOGIE E PRODOTTI DUAL-USE

Processi di R&S dual-use e/o di trasferimento di tecnologie e prodotti dual-use comportano diverse complessità e realizzazioni organizzativo-gestionali anche a seconda delle barriere al trasferimento e alla direzione di questo ultimo, dei soggetti coinvolti e delle tecnologie e prodotti oggetto di trasferimento. Considerando una definizione già riportata e di compromesso tra le diverse fonti analizzate, nella espressione "tecnologie e prodotti" sono inclusi anche ricerca, conoscenza codificata (es. brevetti, e in generale informazioni specifiche necessarie a sviluppo, produzione e utilizzo, inclusi dati tecnici e assistenza tecnica)[79] e know-how, principi e tecniche di management per la gestione dei processi di R&S e di produzione, componenti, servizi, software.

Come visto, le politiche sul dual-use possono spaziare da quelle più focalizzate sulla R&S dual-use intesa come tale fin dall'inizio a quelle, maggioritarie, che hanno come obiettivo il miglioramento del trasferimento tecnologico dual-use, quindi la diffusione di tecnologie e prodotti dual-use in applicazioni nel settore inverso. Emerge comunque chiaramente, secondo diverse opinioni che, indipendentemente dalle tipologie di meccanismi di R&S e/o trasferimento applicabili, conta molto anche la mentalità aziendale: se il processo è strutturato e documentato si favorisce il successo dell'iniziativa, ma è essenziale che sia creata la cultura professionale adeguata.

Non è agevole dunque determinare quali meccanismi di R&S siano più performanti, perché la valutazione varia in funzione del tipo di organizzazione che vuole realizzare R&S e trasferimento e degli aspetti sopra menzionati. Le condizioni variano da caso a caso e, come vedremo, mentre alcune dinamiche di trasferimento sono più basate su tecnologie e prodotti, altre sono più improntate ad una modifica strutturale della maniera in cui processi di R&S e di produzione civili/sicurezza e militari possono interagire.

Seguendo ed adattando l'impostazione di alcuni autorevoli autori citati, come Jordi Molas-Gallart, nella *Guide for Regions and SMEs - EU Funding for Dual-use* edita nel 2014 dalla CE, si può ritenere che processi di R&S e/o trasferimento avvengano internamente quando tecnologie e prodotti sviluppati per una determinata business unit per scopi militari vengono poi utilizzati nella stessa azienda all'interno di una diversa business unit per scopi civili/sicurezza (o viceversa). Alternativamente, il trasferimento può avvenire esternamente tra unit di differenti aziende o all'interno di differenti business unit della stessa corporate.

I trasferimenti (sia interni che esterni) si distinguono anche in base alla necessità o meno di adattamenti nel passaggio ad applicazioni del settore inverso. L'adattamento può

[79] Cattani, G. e Paolucci, P. M. (2015), "L'esportazione dei beni dual-use. Manuale teorico-pratico", Maggioli Editore, p. 38

riguardare tecnologie e prodotti oggetto di trasferimento (es. cambiamenti tecnici nelle caratteristiche o nell'interfaccia di tecnologie e prodotti), ma anche la struttura dell'azienda e/o i processi della business unit (incluse competenze del personale) come, rispettivamente, nel caso di un'azienda che crei nuove business unit o le elimini (ad esempio a seguito di processi di diversificazione o conversione), o che modifichi processi di R&S di business unit già esistenti (ad esempio a seguito di processi d'integrazione civile-militare di attività di R&S). Il trasferimento e l'eventuale processo di adattamento - ove presente possono, pertanto, riguardare tutti i suddetti aspetti nel passaggio da applicazioni civili/sicurezza a militari, o viceversa. Nei casi di trasferimento descritti, possono esserci costi economici e di transazione che saranno maggiori nel caso in cui intervenga l'adattamento, ad esempio, a seguito di nuovi e differenti requisiti cui una tecnologia deve rispondere o derivanti da trasformazioni aziendali che implicano nuove complessità tecnico-gestionali. I costi di trasferimento con adattamento potrebbero, a seconda dei casi, risultare comunque minori rispetto allo sviluppo *ex novo* di una tecnologia o prodotto.

Un esempio di meccanismo per trasferimento interno diretto (senza adattamento) potrebbe essere la creazione di database centralizzati relativi a tecnologie e prodotti in via di sviluppo o sviluppati internamente ad un'azienda e contenenti informazioni tecniche, a cui le varie unit civili/sicurezza o militari dell'azienda possano accedere e che faciliterebbero l'individuazione di tecnologie e prodotti validi per funzioni del mercato inverso. Un database di tale tipo avrebbe un impatto positivo per grandi aziende (che ne possono sostenere costi e aggiornamento), mentre PMI potrebbero utilmente avvalersi di workshop interni. Il trasferimento interno diretto è tipico anche di prodotti e componenti COTS/NDI.

I meccanismi di R&S e/o trasferimento interno con adattamento riguardano tecnologie che necessitano di cambiamenti tecnici o che ne implicano all'interno dell'organizzazione. Questi possono includere, ad esempio, attività congiunte di R&S tra ambiti civile/sicurezza e militare con l'obiettivo di generare spillover di conoscenze trasferite internamente all'azienda, nell'intero ciclo di vita della tecnologia[80]. Esempi di attività congiunte di R&S potrebbero essere rappresentati dagli elicotteri AW101 (MIL → CIV/SIC) e AW 139 (CIV/SIC → MIL).

Forme di integrazione o concentrazione orizzontale possono essere del tipo conversione che prevede l'abbandono di un tipo di mercato (tradizionalmente il militare) o del tipo diversificazione, che prevede una estensione delle attività anche al mercato inverso (verso nuovi clienti o verso nuovi prodotti o verso entrambe le direzioni). La diversificazione,

[80] Fan, J. e Hou, G. (2009), "Research on Integration Platform of Dual-use Core Technologies Based on Open Innovation", International Conference on Management Science & Engineering, 14-16 Settembre, p. 1632

a sua volta, può avvenire attraverso crescita interna (ad esempio con creazione di una business unit che si occupi di sviluppare e commercializzare le tecnologie per un settore differente da quello di origine) o tramite crescita esterna (ad esempio attraverso acquisizioni di aziende operanti nel mercato inverso). Un esempio di diversificazione tramite crescita interna potrebbe essere rappresentato dalla Iveco Defence Vehicles (Iveco DV) nel campo dei veicoli da trasporto (CIV/SIC → MIL).

Nel trasferimento esterno diretto rientrano la vendita o concessione in licenza di brevetti. In tali casi, sul trasferimento di tecnologie e prodotti possono impattare le conoscenze tacite degli sviluppatori che non possono essere sostituite dal solo brevetto. Oltre la definizione di diritti di proprietà intellettuale pronti per la vendita o la concessione in licenza, dovrebbero, infatti, aggiungersi impegni su conoscenze collegati al contratto di cessione[81]. Nel trasferimento esterno diretto possono rientrare prodotti e componenti COTS/NDI. Un esempio di trasferimento esterno diretto tramite COTS potrebbe essere rappresentato dal Condor Cluster un network di oltre 1,760 console PlayStation 3 (PS3) realizzato nel 2010 dalla US Air Force per formare un "supercomputer" a sostegno delle proprie operazioni aeree (CIV/SIC → MIL).

Nel trasferimento esterno con adattamento possono rientrare forme di partnership civile/sicurezza-militare, spin-in/spin-on, spillover tecnologici. Un esempio di partnership civile/sicurezza-militare, come programma di R&S, potrebbe essere rappresentato da COSMO SkyMed che costituisce un caso di processo di sviluppo interamente pensato come dual-use e portato avanti congiuntamente dalla Difesa e dall'Agenzia Spaziale Italiana (ASI). Esempi di spin-in/spin-on come trasferimento esterno (diretto, cioè senza adattamento da parte di chi cede o con adattamento) potrebbero essere presenti nel velivolo da combattimento multiruolo F-35 JSF (CIV/SIC → MIL) e nel programma FALCON (CIV/SIC → MIL)[82]. Spin-in/spin-on possono aver luogo anche tra diverse business unit all'interno alla

---

[81] Bellais, R. e Guichard, R. (2006), "Defense innovation, technology transfers and public policy", Defence and peace economics

[82] Il Falcon è un sistema di comunicazione tattica, attivo quindi principalmente all'interno del teatro delle operazioni, utilizzato dall'esercito e dall'aeronautica militari del Regno Unito. Il sistema è stato sviluppato e prodotto dall'industria della difesa britannica BAE Systems, sulla base di un contratto siglato nel 2006, con il primo impiego in operazioni nel 2014 (Army Technology 2016). Il sistema permette la trasmissione di audio, dati e immagini tra una serie di elementi messi in rete, inclusi quartier generali, posti di comando e veicoli. Per quanto riguarda l'applicazione, non si può parlare di dualità in quanto è utilizzato dalle forze armate britanniche per operazioni militari. Dal punto di vista tecnologico, Falcon è basato interamente su Internet Protocol (IP) standard, una scelta che all'inizio poteva apparire ambiziosa, ma che si è rivelata di successo tanto che lo stesso percorso è stato intrapreso poi per altri sistemi. Lo scambio di dati basato su IP è comunque gestito con un elevato livello di sicurezza specifico per le forze armate britanniche: ad esempio, Falcon distingue le informazioni in 4 livelli di segretezza e le distribuisce solo ai destinatari che hanno l'autorizzazione ad accedere al livello di segretezza richiesto dalla specifica informazione. In questo senso si può parlare di dualità di tecnologia, in quanto l'ICT alla base del Falcon è la stessa parte della rete internet civile. Anche grazie a ciò, a sua volta Falcon è in grado di interfacciarsi con altri sistemi di comunicazione militari e civili. Vista l'importanza dell'addestramento del personale militare deputato all'utilizzo del sistema, nel 2015 il Ministero della Difesa britannico ha siglato un contratto da 6,4 milioni di sterline con BAE Systems per un servizio completo di training sull'uso del Falcon per i successivi quattro anni e mezzo.

stessa azienda e configurare dunque un trasferimento interno. Un esempio di spin-in/spin-on come trasferimento interno con adattamento da parte di chi cede potrebbe essere rappresentato dall'aeromobile a pilotaggio remoto (APR) Falco (MIL → CIV/SIC). Un esempio di spillover tecnologico potrebbe essere rappresentato dal "Foxhound" Light Protected Patrol Vehicle (CIV/SIC → MIL)[83].

TECHNOLOGY BROKERING OFFICE INTERNO

R&S dual-use e trasferimento di tecnologie e prodotti dual-use, interni od esterni, diretti o indiretti, possono essere facilitati dall'operato di un technology brokering office interno all'azienda che agisca come competenza di interfaccia, come analista delle tecnologie per intuire le potenziali applicazioni in settore inverso. Il tecnologo deve potere e sapere osservare cosa l'azienda, la business unit sa fare e come lo fa (processi), per valutare opportunità di sviluppo ed utilizzo nel mercato inverso[84].

Questa figura rappresenta un costo per l'azienda, ma può portare vantaggi, tramite la ricerca di trasversalità di applicazione di tecnologie e prodotti da un settore a quello inverso e la relazione con strutture di brokeraggio private o istituzionali esterne all'azienda. Un technology brokering office interno all'azienda rappresenterebbe una soluzione particolarmente appropriata per organizzazioni di grandi dimensioni, generalmente caratterizzate da limitata circolazione interna di idee, siti separati, forte specializzazione senza rotazione negli incarichi. Questo ruolo risulterebbe dunque tanto più utile quanto più le dimensioni dell'azienda e le complessità dei prodotti che sviluppa, crescono. Per le PMI invece, che generalmente hanno organizzazioni minimali, potrebbero funzionare meglio la condivisione spontanea in workshop, senza costi aggiuntivi. Vicino alla figura del technology brokering office interno all'azienda è suggerita da alcuni l'idea di prevedere, in modello matriciale, una funzione aziendale specifica dedicata alla ricerca sistematica di trasversalità di applicazione da un settore all'altro a livello di tecnologie e prodotti[85].

---

[83] Ocelot/Foxhound è il veicolo leggero da pattugliamento dell'esercito britannico, in produzione dal 2011 per sostituire, con 400 previste unità, lo Snatch Land Rover. È stato commissionato dalla Gran Bretagna con il fine di disporre di un mezzo adeguato per le operazioni in Afghanistan, in particolare a protezione da Improvised Explosive Devices (IEDs). Il sistema è modulare e permette una sostituzione dei componenti con altri tecnologicamente sviluppati su standard internazionali anche da produttori diversi. Il Foxhound, può essere fornito di sistemi d'arma (es. mitragliatrice), ma resta fortemente versatile. Infatti, non essendo dotato di sedili fissi, il veicolo può essere impiegato in operazioni militari come ambulanza, come mezzo di trasporto, e come mezzo di supporto per le attività di comando e controllo nel corso di operazioni a livello tattico (General Dyanmics Land Systems 2016). Dal punto di vista tecnologico vi è una significativa dualità, dovuta allo spillover dal civile al militare. Lo sviluppo tecnologico e l'industrializzazione del Foxhound sono infatti condotti dalla statunitense General Dynamics Land Systems – Force Protection Europe. Nella progettazione del motore e della piattaforma ha avuto invece un forte ruolo la Ricardo, società di consulenza ingegneristica (Hopperton 2012) nella quale dunque si è verificato uno spillover tecnologico (incluso know-how) da investimenti in R&S effettuati nell'ambito delle attività civili (in particolare motori sportivi), preponderanti nella società, ad applicazioni in ambito difesa, area tradizionalmente trattata dalla Ricardo.

[84] Nones, M. (2019), "L'innovazione tecnologica nei settori civile e militare", p.151

[85] Mérindol, V. e Versailles, D. W. (2014), "La dualité dans les entreprises de Défense", p. 50

SETTORE PUBBLICO

DOMANDA

La domanda influenza lo sviluppo e diffusione di tecnologie e prodotti dual-use in base al livello di frammentarietà, sia dal punto di vista della varietà di stakeholder attivi in maniera diretta ed indiretta nella sua formulazione che dal punto di vista di quelli coinvolti nel finanziamento della stessa, con ruoli di user e buyer che non sempre coincidono. La frammentarietà della domanda è un'incognita che l'azienda deve valutare e gestire ed ha sempre un impatto negativo, anche su R&S dual-use e/o trasferimento di tecnologie e prodotti dual-use. Per il soggetto pubblico, la frammentarietà può non nascere solo da una mancata o errata pianificazione degli investimenti, quanto dalla incertezza sulla disponibilità a lungo termine degli stessi.

Il mercato militare è secondo alcuni caratterizzato da un grado di frammentarietà della domanda minore rispetto al mercato civile/sicurezza e sostanzialmente riguarda per la parte pubblica i MDIF e, per la parte privata, le private military companies. Secondo altri, invece, il mercato militare, nonostante i volumi non siano paragonabili a quelli del mercato inverso, ha un grado di frammentazione a causa della elevata customizzazione dei sistemi per ogni cliente.

Il mercato civile/sicurezza include a livello pubblico la domanda generata dai MINT e da "agenzie di sicurezza" di varia natura, oltre quella generata da private/public companies che forniscono un servizio pubblico (es. aeroporti); a livello privato include clienti privati singoli o private companies per la protezione propria o della propria attività[86]. Ad esempio, in Italia nella domanda pubblica oltre alle Forze di Polizia, i Vigili del Fuoco, il Corpo Forestale dello Stato e la Guardia di Finanza, rientrano in generale gli Enti coordinati dal Dipartimento della Protezione Civile. Tra i Ministeri con attività operative di interesse per la sicurezza interna rientrano anche Ministeri, ad esempio, in materia di Ambiente e Salute. Oltre ad Enti locali, quali Regioni e Comuni, che partecipano anch'essi alla formazione della domanda pubblica di assetti di sicurezza. Il mercato civile/commerciale è ancor più frammentato perché i requisiti sono determinati dall'industria stessa cercando di individuare i bisogni del cliente.

Nel settore militare, la domanda pubblica viene definita attraverso procedure formalizzate che fissano esigenze operative (operational needs) e funzioni associate al soddisfacimento delle stesse poi specificate in requisiti tecnici (operational requirements).

[86] IRIS, IAI, MIIR (2010), "Study on the industrial implications in Europe of the blurring of dividing lines between security and defence", p. 63

Questo avviene sulla base di un'analisi delle capacità dello strumento militare, in cui vengono indicate quali tecnologie sono necessarie per coprire eventuali gap capacitivi "funzionali" (technology-oriented approach). Nel settore civile/sicurezza può essere invece diffusa una formulazione della domanda pubblica che indichi non già le tecnologie adatte alle funzioni, ma le esigenze operative e funzioni da soddisfare (mission/application-oriented approach). Tali differenti modalità (o in alcuni casi lato civile/sicurezza mancanza di processi formalizzati per la definizione della domanda e mancanza di cultura del procurement) impattano in maniera diversa sulla formulazione della domanda e sulla possibile emersione di un mercato di tecnologie e prodotti dual-use.

Secondo alcuni, tecnologie e prodotti dual-use – rappresentati come area comune tra i mercati civile/sicurezza e difesa – potrebbero favorire una maggiore aggregazione della domanda, in particolare pubblica, così mitigando i livelli di frammentarietà che caratterizzano i mercati civile/sicurezza e civile/commerciale. Resta fermo che tale possibilità va verificata segmento per segmento perché la realizzazione dipende dai singoli casi, ciascuno con un TRL ottimale diverso, nell'intersezione tra i due mercati.

ESIGENZE, FUNZIONI E REQUISITI

Come riportato nel precedente paragrafo, esigenze operative e funzioni sono dunque entrambi elementi che contribuiscono alla definizione ed espressione della domanda di mercato. Nella domanda militare pubblica, le soluzioni sono stabilite tramite documenti di specificazione tecnica che individuano requisiti tecnici (operational requirements). Questi in Italia sono divisi in Requisiti Operativi Preliminari (ROP), che servono ad identificare e restringere il campo delle possibili soluzioni, e Requisiti Operativi Definitivi (ROD), che vengono usati per formulare i contratti di acquisto e quindi stabilire esattamente le specifiche tecniche e che sono alla base delle attività industriali volte al soddisfacimento degli stessi.

Vi sono, dunque, due momenti distinti: la definizione di esigenze operative e funzioni, e la formulazione di requisiti tecnici che si possono distinguere in requisiti funzionali e non funzionali. I requisiti tecnici funzionali rappresentano le funzioni che la tecnologia e i sistemi devono fornire per soddisfare l'esigenza operativa degli end-user nei diversi ambiti civile/sicurezza o militare. I requisiti tecnici non funzionali possono riguardare proprietà del tipo usabilità, robustezza e prestazioni dei materiali, affidabilità, rispondenza a standard e requisiti di rilascio. Secondo alcuni, i requisiti non funzionali sono essenziali perché, quanto i requisiti funzionali, impattano sulla capacità di sviluppare e/o adattare tecnologie e prodotti

per rispondere ai bisogni dei clienti del mercato inverso e ad essi è legata una rilevante parte di costi di progettazione e di produzione[87].

CONOSCENZA TECNOLOGIA

I mercati civile/sicurezza e militare presentano livelli di conoscenza e accesso a tecnologie e prodotti disponibili o in via di sviluppo e di conoscenza di potenziali applicazioni anche molto diversi tra loro. Infatti, mentre in ambito civile/sicurezza solitamente l'azienda non ha restrizioni (contrattuali e di opportunità) per pubblicizzare proprie tecnologie e prodotti, in ambito militare la diffusione della conoscenza delle caratteristiche di una tecnologia o di un prodotto può costituire un fattore di rischio per il vantaggio competitivo e può essere escluso da obblighi contrattuali di riservatezza imposti dal committente. Il problema si pone anche all'interno del solo ambito militare. Come osservato da alcuni, anche se la segretezza rimane una caratteristica chiave della R&S in ambito difesa, classificare tutto non sembra opportuno perché non tutte le informazioni sono sensibili ed è sensato trovare una misura per non limitare l'interazione tra i membri della comunità del settore di cui beneficiano anche le stesse FFAA per il ritorno sugli investimenti in R&S[88].

Esistono strumenti di politica industriale e tecnologica che possono favorire conoscenza e accesso a tecnologie e prodotti disponibili e conoscenza di potenziali applicazioni e, dunque, favorire l'incontro tra domanda e offerta dei diversi settori civile/sicurezza e militare e la possibilità di modelli di open innovation. Nel Capitolo 3 saranno analizzati strutture di technology brokering esterne all'aziende, cluster tecnologici/industriali, database industriale europeo dual-use e database industriale europeo sulle tecnologie critiche. Tali strumenti devono gestire il diverso timing dell'espressione della domanda e la rapida evoluzione tecnologica. Si tratta di strumenti coinvolti nel monitoraggio tecnologico in cui rientrano attività che analizzano l'evoluzione dell'innovazione in ambiti tecnologici di interesse con varie finalità che dipendono anche dalla natura dei soggetti coinvolti.

Anche le aziende possono avere un ruolo attivo nelle attività di monitoraggio tecnologico per loro obiettivi, come pure partecipare in cluster o interagire con technology brokering office esterni. Tali strumenti possono favorire l'incontro tra domanda e offerta, ma anche la circolazione di conoscenza tra aziende[89]. Tra gli obiettivi del monitoraggio tecnologico si possono, infatti, trovare l'acquisizione di nuove tecnologie tramite vendita o

---

87 Mérindol, V. e Versailles, D. W. (2014), "La dualité dans les entreprises de Défense", p. 45

88 Bellais, R. e Guichard, R. (2006), "Defense innovation, technology transfers and public policy", p. 277

89 Georghiou, L., Edler, J., Uyarra, E. e Yeow, J. (2014), "Policy instruments for public procurement of innovation: Choice, design and assessment", Technological Forecasting and Social Change

concessione in licenza di brevetti, la valutazione del livello tecnologico raggiunto dai competitor e l'identificazione delle traiettorie di sviluppo del mercato. Le attività di monitoraggio tecnologico sono molto utili a modelli di open innovation e all'individuazione di brick di tecnologie emergenti.

Il monitoraggio tecnologico viene condotto attraverso una pluralità di strumenti, dalla semplice lettura e analisi di pubblicazioni scientifiche, ai contatti con i dipartimenti di R&S delle imprese, al monitoraggio di banche dati di brevetti. Quest'ultimo caso, che rappresenta lo strumento principale per il monitoraggio tecnologico su larga scala, presenta sfide significative dovute all'inesistenza di una banca dati unica, all'alto numero dei dati da analizzare e alla mancanza di uniformità nella formulazione dei brevetti. Vi sono numerose banche dati per i brevetti, sia nazionali che internazionali, che spesso si sovrappongono, che possono contenere duplicazioni degli stessi brevetti perché non hanno necessariamente gli stessi standard di ricerca e di dettaglio. Esistono infatti imprese e consorzi specializzati nel fornire assistenza in tali attività.

GOVERNANCE FINANZIAMENTI PUBBLICI

L'eterogeneità degli stakeholder coinvolti nei processi di innovazione dual-use, il numero e la tipologia degli strumenti di finanziamento e la varietà di istituzioni ed enti preposti alla loro gestione rende il quadro in materia di ricerca dual-use complesso.

LIVELLO UE

A livello UE, ad esempio, la parziale sovrapposizione dei mandati delle istituzioni e delle relative iniziative, spesso con differenti modalità di gestione dei programmi, può dar luogo a divergenze sulle priorità di finanziamento e duplicazioni con costi economici ed inefficienze. Su tale situazione impatta anche la divergenza tra approcci intergovernativi (EDA) e sovranazionali (CE) per cui, accanto alle riflessioni sull'efficacia e l'efficienza di determinati programmi di finanziamento per R&S e alla valutazione sulle priorità tecnologiche e industriali, vi sono forma mentis e tendenze strutturali che condizionano il comportamento dei vari attori rispetto al tema del dual-use.

Collaborazione tra EDA e CE

Per favorire il coordinamento fra EDA e CE, nel 2009 è stato creato uno European Framework Cooperation (EFC) for Civilian Security Space and Defence-Related Research, avente lo scopo di assicurare sistematicamente il coordinamento degli investimenti in R&S separatamente gestiti da EDA, CE e European Space Agency (ESA) con particolare

attenzione alle aree del dual-use, al fine di evitare duplicazioni. Tra le aree considerate, lo EFC individuava nella gestione di eventi CBRN una priorità per gli investimenti europei. Nel 2010, l'EDA ha inaugurato un Joint Investment Programme CBRN (JIP CBRN) che ha poi favorito l'istituzione di un ulteriore EFC specifico per le minacce CBRN[90]. Tra il 2012 e il 2013, il JIP ha finanziato in totale 14 progetti per un valore complessivo di 12 milioni di euro corrisposti da 12 Stati membri EDA e dalla Norvegia[91].

La collaborazione di CE e EDA nella governance dei programmi di finanziamento, e quindi a proposito di sinergie e influenza su R&S e/o trasferimento di tecnologie e prodotti dual-use, è proseguita con il Pilot Project (PP) for research in the field of Defence del 2015, nel contesto del quale l'Agenzia era responsabile per l'amministrazione dei finanziamenti provenienti dal budget europeo, previsti da un Delegation Agreement con la CE[92]. Il PP è stato esteso fino al 2018 fornendo 1.4 milioni di euro per coprire i costi di tre progetti: Inside Building Awareness and Navigation for Urban Warfare (SPIDER), Unmanned Heterogeneous Swarm of Sensor Platforms (EuroSWARM) e Standardisation of Remotely Piloted Aircraft System (RPAS) Detect and Avoid (TRAWA), ciascuno dei quali ha ricevuto un finanziamento di circa 433,000 euro[93].

Il PP è stata una innovazione importante che è poi evoluta, nel 2017, nella creazione della Preparatory Action on Defence Research (PADR), tramite cui nel periodo 2017-2019 sono stati finanziati 18 progetti per un budget complessivo di oltre 90 milioni di euro. In tale contesto, la CE era responsabile per l'implementazione del programma, mentre la valutazione dei progetti e l'attuazione di alcuni obiettivi specifici erano delegati all'EDA[94]. In ambito European Defence Industrial Development Programme (EDIDP), gestito direttamente dalla CE, il ruolo dell'Agenzia è stato ridimensionato a membro osservatore nel comitato di supporto. Per tale progetto il finanziamento totale è stato di circa 500 milioni di euro a supporto della ricerca e sviluppo della difesa europea nel periodo 2019-2020[95]. In H2020, l'Agenzia aveva status da osservatore nei Comitati di programma. In Horizon Europe, tale condizione dell'EDA è rimasta nel solo ambito del comitato dell'EDF[96]. Un elemento significativo, se si considera che il Trattato di Lisbona attribuisce il compito di

---

90 EDA, "CBRN JOINT INVESTMENT PROGRAMME"; EDA (2011), "EDA and the Commission signed a European Framework Cooperation coordination letter yesterday", 16 Settembre

91 EDA, "Joint Investment Program on CBRN Protection"

92 EDA (2016), "Call for proposals for the Pilot Project on defence research", 13 Maggio

93 EDA (2016), "First EU Pilot Project in the field of defence research sees grant agreements signed for €1.4 million", 28 Ottobre

94 CE, "Preparatory Action on Defence Research (PADR)"

95 PE e Consiglio dell'UE (2018), "Regolamento (UE) 2018/1092 che istituisce il programma europeo di sviluppo del settore industriale della difesa, volto a sostenere la competitività e la capacità di innovazione dell'industria della difesa dell'Unione", 18 Luglio; CE, "European Defence Industrial Development Programme (EDIDP)"

96 PE e Consiglio Dell'UE (2021), "Regolamento (UE) 2021/697 che istituisce il Fondo europeo per la difesa e abroga il regolamento (UE) 2018/1092", 29 Aprile

supportare la ricerca e lo sviluppo delle capacità militari all'EDA, sottoposta all'autorità del Consiglio.

Implicazioni del ruolo della CE

Negli ultimi anni si osserva un crescente ruolo della CE con impatti anche sui processi decisionali, ad esempio passati da intergovernativo a sovranazionale nel contesto dell'EDAP, presentato dalla CE nel 2016. L'EDAP ha permesso alla CE di (co-)finanziare progetti di ricerca e acquisizione tramite il bilancio comunitario[97]. L'impatto di tale sviluppo risulta evidente se si considerano i finanziamenti previsti dall'EDF, 8 miliardi tra il 2019 e il 2020, e li si paragona agli 1.1 miliardi di euro investiti dall'EDA dal 2004 al 2019[98]. L'EDF ha infatti introdotto nell'ambito della governance dei finanziamenti europei una assoluta novità includendo un decision-making sovranazionale in un settore, quello della Politica di sicurezza e di difesa comune (PSDC), tradizionalmente intergovernativo[99].

Nonostante il progressivo coinvolgimento della CE nel settore sia limitato dall'Art. 41.2 del Trattato sul funzionamento dell'Unione europea (TFUE), che impedisce l'utilizzo del bilancio comunitario per operazioni con implicazioni militari o relative alla difesa[100], la CE ha giustificato i propri investimenti nel settore con motivazioni economiche, affermando che la ricerca nel campo della difesa contribuisce alla creazione di valore e alla competitività delle imprese[101]. Considerare che parte del mercato della difesa abbia natura dual-use permette alla CE di svolgere un ruolo più efficace nel pretendere minori eccezioni alle regole del mercato unico – cioè minore invocazione da parte degli Stati membri dell'Art. 346 del TFUE. È, infatti, sempre meno giustificabile per i Paesi sostenere che i loro programmi di sviluppo delle capacità non riguardino anche tecnologie e prodotti civili, quindi rientranti nelle normali condizioni del mercato unico[102]. Si potrebbe affermare che la CE considera il settore della sicurezza e difesa un'ulteriore componente dell'integrazione europea, alla quale estendere una governance basata sul Trattato volta a rafforzare il mercato interno unico, in una logica di concorrenza, efficienza ed innovazione[103].

La crescita delle competenze e dell'influenza della CE – e delle istituzioni europee in generale – nel campo della difesa non è visto positivamente da diversi Stati membri che,

---

97 Lavallée, C. (2018), "The European Commission: An Enabler for the European Security and Defence Union", Real Instituto Elcano

98 Haroche, P. (2020), "Supranationalism strikes back: a neofunctionalist account of the European Defence Fund", Journal of European Public Policy, 2 Giugno

99 Ibid.

100 Gazzetta ufficiale dell'UE, "Trattato sull'Unione europea (versione consolidata)"

101 Haroche, P. (2020), "Supranationalism strikes back"

102 Fiott, D. (2015), "European defence-industrial cooperation: from Keynes to Clausewitz", Global Affairs, p. 162

103 Marrone, A. e Ungaro, A. R. (2014), "Actors in the European defence policy area: roles and developments", IAI e Centro Studi sul Federalismo (CSF), Novembre

nonostante siano favorevoli ad un aumento dei finanziamenti europei per il dual-use, intendono proteggere la propria sovranità in materia di difesa. Il dual-use, infatti, rappresenta un settore strategico per la sicurezza nazionale e risponde ad una logica politica piuttosto che di libero mercato.

Fondi strutturali e di investimento europei

Il livello di complessità del quadro dei finanziamenti pubblici UE potenzialmente validi per R&S dual-use è testimoniato da alcune iniziative istituzionali volte a favorire l'accesso a fondi europei utilizzabili, tra cui due guide pubblicate nel 2014 rispettivamente dall'EDA e dell'allora Directorate-General for Enterprise and Industry (DG-ENTR) della CE. La prima, *Your Guide to European Structural Funds for Dual-use technology projects*, riguarda l'utilizzo degli European Structural and Investment Funds (ESIFs) per progetti tecnologici dual-use[104]. Nel periodo 2014-2020, agli ESIFs erano allocati 454 miliardi di euro, larga parte dei quali destinati allo European Regional Development Fund (ERDF). Nel financial framework successivo il finanziamento è di circa 409 miliardi di euro. La seconda guida, *EU funding for Dual-use: A practical guide to accessing EU funds for European Regional Authorities and SMEs* riguarda l'accesso a varie forme di finanziamento europeo da parte di regioni e PMI a fondi europei per R&S nel settore dual-use[105].

Entrambe le guide prestano particolare attenzione all'ERDF, illustrando le modalità in cui le Regioni possono elaborare strategie su prodotti dual-use nell'ambito delle loro Research and Innovation Smart Specialisation Strategies (RIS3), facilitando così l'accesso a finanziamenti del Fondo. La coerenza del progetto da finanziare con la RIS3 sviluppata dalla Regione è infatti condizione dell'ammissibilità ai finanziamenti. In tal modo, gli ESIFs sostengono trasferimenti di tecnologia, creazione di prototipi, diffusione delle innovazioni ed elementi simili, che aiutano le aziende a diversificare verso il mercato inverso[106].

Per comprendere le potenzialità degli ESIFs, in particolare dell'ERDF, in materia di ricerca dual-use, è utile considerare a titolo esemplificativo il caso della Regione Lazio, che ha ricevuto finanziamenti dall'ERDF per circa mezzo miliardo di euro nel periodo 2014-2020, di cui circa il 30% impiegato in attività di R&S[107]. Tali investimenti hanno riguardato sette Aree di Specializzazione (AdS) individuate a livello regionale: aerospazio, agrifood, green economy, industrie creative e digitali, patrimonio culturale e tecnologie per la cultura,

[104] EDA (2014), "Your Guide to European Structural Funds for Dual-use technology projects"
[105] DG-ENTR (2014), "EU funding for Dual-use: A practical guide to accessing EU funds for European Regional Authorities and SMEs"
[106] CE (2015), "Helping SMEs tap into EU funding for dual-use projects", 22 Giugno
[107] CE, "ROP Lazio ERDF"

scienze della vita, sicurezza. L'AdS Aerospazio, che opera in forte sinergia con l'AdS Sicurezza, ha ricevuto il 14% del totale dei finanziamenti a disposizione, concentrandosi sulle tematiche "aerospazio e sicurezza" e "tecnologie abilitanti-KETs", rispettivamente con 13 e 11 progetti finanziati[108]. Le traiettorie tecnologiche prevalenti all'interno dei progetti finanziati relativi all'AdS Sicurezza riguardano la "digital e cyber security" (10 progetti per un valore di 3.4 milioni di euro) e la "resilienza ai disastri naturali" (8 progetti finanziati per un valore di 1.8 milioni di euro)[109]. Nel contesto della RIS3 2014-2020, la natura dual-use delle AdS Sicurezza e Aerospazio era dimostrata dall'individuazione dell'area CBRN/dual-use quale settore di particolare interesse, in termini di cross-fertilisation, per l'AdS Aerospazio[110]. Per quanto concerne l'AdS Sicurezza, invece, la dimensione dual-use era testimoniata dal ruolo primario rivestito, in questa area, dai centri militari coinvolti[111]. Per il periodo 2021-2027, nell'ambito della revisione della propria RIS3, la Regione Lazio ha deciso di introdurre due nuove AdS: Automotive e Economia del Mare[112]. La dimensione dual-use di queste AdS risulta rilevante soprattutto se si considera che una delle traiettorie di sviluppo individuate dal piano d'azione triennale Cluster Tecnologico Nazionale (CTN) Blue Italian Growth (BIG) riguarda la cantieristica e la robotica marina, inclusi sistemi dual-use per la Difesa[113].

A livello Europeo, nel periodo 2014-2020, gli ESIFs hanno finanziato circa 972 progetti dual-use (il 58% del totale dei progetti) o relativi al settore della difesa, per un totale di oltre 1 miliardo di euro (oltre 860 milioni di co-finanziamento da altri canali prevalentemente privati)[114]. Questi investimenti nel settore dual-use e della difesa provengono principalmente dall'Erdf (814 milioni), con un importante contributo anche dello European Social Fund (ESF) (118 milioni) e dai programmi della European Territorial Cooperation (ETC) (33 milioni).

Ulteriori linee di finanziamento

Nel quadro della CE, nel 2016 è stato istituito lo European Network of Defence-related Regions (ENDR)[115] finalizzato ad incoraggiare attività dual-use nel settore della difesa tra autorità, cluster e compagnie regionali. A livello italiano ne fanno parte il Distretto Tecnologico Aerospaziale della Campania (DAC) e l'Umbria Aerospace Cluster.

---

108 Regione Lazio, "Lazio Smart Verso la nuova Strategia di Specializzazione Intelligente del Lazio"
109 Ibid.
110 Regione Lazio, "Smart Specialization Strategy (s3)"
111 Ibid.
112 Regione Lazio, "Lazio Smart Verso la nuova Strategia di Specializzazione Intelligente del Lazio"
113 Ibid.
114 CE (2021), "Study on the Contribution of the defence sector to Regional Development through the European Structural and Investment Funds", 6 Maggio
115 ENDR, "European Network of Defence-Related Regions"

Alle due guide del 2014 è seguita la pubblicazione di altre due guide da parte della CE, nel 2017[116]: *Dual use technology in the EU - Helping smes bring innovation to market* e *Dual-use Technologies: EU funding opportunities*, mirate rispettivamente a coinvolgere maggiormente le PMI nella realtà dual-use europea e fornire indicazioni pratiche sulle opportunità di finanziamento europeo per attività concernenti tecnologie e prodotti dual-use.

Nel periodo 2021-2027, sono stati allocati circa 2 miliardi di euro all'Internal Security Fund (ISF) a fronte dei circa 4 miliardi devoluti nel periodo 2014-2020[117]. Tale fondo risulta di interesse poiché mira a garantire l'interoperabilità dei sistemi informativi, proteggere le infrastrutture critiche e finanziare l'acquisto o lo sviluppo, di infrastrutture per la sorveglianza dei confini[118]. Il piano nazionale per l'utilizzo di questi fondi prevedeva, nel periodo 2014-2020, l'allocazione di circa il 20% dei fondi ad iniziative che promuovessero la prevenzione di crisi ed emergenze in materia di CBRN, cybercrime, sicurezza alimentare e protezione delle infrastrutture critiche informatiche[119].

Per contribuire a delineare le fonti di investimento disponibili a livello UE, l'EDA ha creato lo European Funding Gateway For Defence (EFGD) identificando 26 possibili linee di finanziamento pubblico europeo per enti che operano nel settore della difesa. Tra queste, tre risultano accessibili da enti che operano nel campo del dual-use[120]. La prima è la Connecting Europe Facility (CEF), uno strumento di finanziamento mirato alla promozione della crescita, dell'occupazione e della competitività europea attraverso azioni di rafforzamento intersettoriale che, tramite la messa in comune di risorse finanziarie, tecniche e/o umane, possono contribuire a migliorare l'efficienza dei finanziamenti europei[121]. Il bando della CEF, pubblicato nel 2021, prevedeva una dotazione di 330 milioni di euro dedicati a progetti di mobilità dual-use a cavallo tra il settore civile/sicurezza e quello militare (su un totale di circa 7 miliardi di investimenti)[122]. La seconda linea consiste nella European Investment Bank (EIB) che, siglando un accordo con l'EDA, nel 2018, ha approvato la creazione della European Security Initiative, dimostrando un rinnovato impegno nell'ambito della ricerca, sviluppo e innovazione dual-use[123]. Ciò è reso possibile dal Cooperative Financial Mechanism (CFM), uno strumento preposto allo sviluppo di tecnologia militare, nel contesto del quale la EIB si occupa specificatamente dello sviluppo di prodotti e tecnologie

[116] CE (2017), "Dual-Use technology in the Eu. Helping SMEs bring innovation to market" e Anciaux, P. (2017), "Dual-use technologies: Eu funding opportunities", 31 Marzo
[117] CE, "Internal Security Fund – Performance"
[118] CE, "Internal Security Fund – Annex 3 - Programme performance overview"
[119] MINT, "Programma Nazionale ISF 2014-2020"
[120] EDA, "Eu funding"
[121] CE, "Meccanismo per collegare l'Europa"
[122] Ministero delle Infrastrutture (2021), "Informativa Bando CEF 2021"
[123] EIB (2018), "EIB and European Defence Agency sign cooperation agreement", 28 Febbraio

con applicazioni nel settore civile/sicurezza[124]. Infine, Horizon Europe – e più precisamente i pilastri I (Excellent Science), II (Global Challenges & European Industrial Competitiveness), di cui fa parte il Cluster Civil Security for Society, e III (Innovative Europe) – pubblica calls for proposals per progetti che riguardano l'applicazione di prodotti e tecnologie dual-use nel settore civile/sicurezza.

LIVELLO UE/LIVELLO NAZIONALE

Anche per quanto riguarda l'Italia, la governance dei finanziamenti pubblici per attività di innovazione dual-use è resa complessa dalla compresenza di numerose amministrazioni, centrali e periferiche (regionali, locali). Permane il rischio di inutili duplicazioni, nonostante alcune iniziative e accordi interministeriali di ricerca volti a mitigarlo.

Anche tra i differenti livelli nazionali, tra questi il livello UE, esiste il rischio di una inutile e dannosa duplicazione degli investimenti pubblici in R&S, a causa di diverse agende e priorità tecnologiche. A ciò si aggiunge la questione della protezione delle industrie nazionali per motivi occupazionali o per tutelare particolari settori tecnologici e, dunque, una generale tendenza a favorire un focus nazionale della catena di approvvigionamento con contractor e sub-contractor nazionali, dovuta a questioni di sicurezza delle forniture[125].

In Italia l'istituzione preposta ad individuare e promuovere progetti di ricerca militare in ambito nazionale e internazionale è il Segretariato Generale della Difesa e Direzione Nazionale degli Armamenti (SGD/DNA) del MDIF, responsabile anche di identificare possibili sinergie con le tecnologie dual-use, ovvero gli aspetti militari delle tecnologie dual-use[126]. Il SGD/DNA utilizza un approccio basato sulla possibilità di impiegare basi tecnologiche derivanti da una matrice di ricerca comune per applicazioni in campo civile/sicurezza, militare e dual-use[127]. All'interno di SGD/DNA, il V Reparto Innovazione Tecnologica fornisce supporto tecnico-amministrativo al SGD/DNA. Il V Reparto si impegna ad applicare un principio di complementarità tra i progetti finanziati tramite PNRM e attività svolte grazie a finanziamenti EDA al fine di ridurre il rischio di inutili e inefficienti duplicazioni.

NORMATIVE

Lo sviluppo e la diffusione di tecnologie e prodotti dual-use sono influenzati dalla conoscenza e compliance aziendale verso il quadro istituzionale e di regolamentazione del

[124] EDA (2019), "Cooperative Financial Mechanism (CFM) ready for signing", 26 Settembre
[125] Europe Economics (2014), "Enhancing support to SMEs", p.13
[126] Salamone, L. V. M., "Il procurement dei servizi di ricerca e sviluppo tecnologico in ambito militare alla luce del Codice dei contratti pubblici e delle leggi speciali", Il Diritto Amministrativo
[127] MDIF, "La Ricerca & Innovazione"

mercato inverso e del mercato dual-use nazionale/europeo/internazionale. Di seguito alcuni temi di rilievo.

EXPORT DUAL-USE

Il regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti dual-use è stato aggiornato con il Regolamento 2021/821. I prodotti dual-use, dettagliati nell'Allegato I, sono definiti come "prodotti, inclusi il software e le tecnologie, che possono avere un utilizzo sia civile sia militare e comprendono i prodotti che possono essere impiegati per la progettazione, lo sviluppo, la produzione o l'uso di armi nucleari, chimiche o biologiche o dei loro vettori, compresi tutti i prodotti che possono avere sia un utilizzo non esplosivo sia un qualsiasi impiego nella fabbricazione di armi nucleari o di altri ordigni esplosivi nucleari"[128].

Secondo dati dell'UE, le esportazioni dual-use extra-UE seguono un trend abbastanza costante per quel che attiene al loro valore. Nel 2019, esse hanno rappresentato 119 miliardi di euro (2.3% del totale delle esportazioni europee[129]). Da ultimo, risulta invece in decremento il numero di autorizzazioni richieste. Secondo alcuni esperti è in realtà molto difficile avere stime esatte perché non tutte le esportazioni di fatto dual-use finirebbero per rientrare formalmente nei controlli, al punto che si potrebbe ipotizzare che il dato vero sia il doppio di quello ufficiale. La circostanza per la quale non tutte le esportazioni dual-use rientrerebbero nel radar nei controlli sarebbe in parte attribuita alla non conoscenza della normativa da parte di aziende, specialmente PMI. A questo si aggiungerebbe che in Italia la violazione del Regolamento è un reato e quindi un ulteriore problema sarebbe nel fatto che le aziende potrebbero ritrovarsi in una situazione in cui una volta acquisita consapevolezza, sarebbero disincentivate per timore di subire conseguenze penali per il pregresso. Secondo alcuni si potrebbe valutare una formale moratoria per il passato che potrebbe aiutare l'emersione di nuovi casi. Questo già avverrebbe, ma su una prassi non formalizzata.

Il nuovo Regolamento introduce ulteriori tipologie di Autorizzazioni generali di esportazione dell'Unione europea (AGEU), volte a transizioni a basso rischio che permettono di ridurre gli oneri amministrativi a carico delle imprese garantendo, al contempo, un adeguato controllo dei prodotti e delle tecnologie dual-use nel processo di

[128] PE e Consiglio dell'UE (2021), "Regolamento (UE) 2021/821 che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso (rifusione)"

[129] CE (2021), "Report on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items", 23 Novembre

esportazione[130]. In particolare, è introdotta un'autorizzazione per "Grandi Progetti" che, tramite una unica licenza, permette l'esportazione specifica (valida per un unico utilizzatore finale o destinatario di un Paese terzo) o globale (valida per le esportazioni verso uno o più utilizzatori finali specifici e/o in uno o più Paesi terzi specifici) di un tipo o una categoria di prodotti dual-use verso uno o più Paesi terzi dove uno o più stakeholder intendono impiegare tali prodotti nell'ambito di uno specifico progetto su larga scala. Viene anche estesa la clausola "catch-all" a prodotti e tecnologie dual-use impiegabili nell'ambito della sorveglianza informatica[131], così permettendo alle autorità degli Stati membri di applicare la normativa anche ad items che non rientrino tra quelli elencati dal Regolamento, se ritenuto che possano essere impiegati per la violazione di diritti umani.

Per quel che riguarda il miglioramento della cooperazione tra le autorità nazionali, si ribadisce il ruolo del Dual-Use Coordination Group (DUGP), presieduto da un rappresentante della CE e composto da un esponente di ciascuno Stato Membro, che incentiva la raccolta e la condivisione di dati tra le autorità nazionali. Il nuovo Regolamento stabilisce che il DUGP sia responsabile dell'implementazione di un nuovo "meccanismo di coordinamento dell'applicazione", preposto al raggruppamento di tutte le autorità degli Stati membri che si occupano di rilasciare le licenze di esportazione, al fine di agevolare la reciproca condivisione di informazioni. La condivisione di informazioni continuerà ad avvalersi della *Relazione al Parlamento europeo e al Consiglio sull'attuazione del Regolamento* – contenente informazioni su concessione di licenze, esecuzione dei controlli, amministrazione, dinieghi e divieti con una nuova frequenza di pubblicazione che passa da ogni tre anni, ad annuale. Per quanto concerne la maggiore attenzione al coinvolgimento del settore privato, il Regolamento ne riconosce la rilevanza, con particolare riferimento alle PMI, sottolineando l'importanza delle loro esigenze di informazione[132]. Come osservato da alcuni, ciò non dovrebbe riguardare soltanto esportatori in senso classico, ma anche accademici e altri esportatori di informazioni tecniche[133].

---

[130] Studio Legale Padovan (2022), "ICP obbligatorio con valutazione da parte di UAMA per la neonata autorizzazione grandi progetti e per AGEU 007", 18 Gennaio; Le AGEU sono concesse a tutti gli esportatori che rispettino le condizioni e i requisiti elencati nelle sezioni da A ad H dell'allegato II.

[131] PE e Consiglio dell'UE (2021), "Regolamento (UE) 2021/821 che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso (rifusione)"

[132] Ivi, Art. 5

[133] Bauer, S. e Bromley, M. (2016), "The dual-use export control policy review: balancing security, trade and academic freedom in a changing world", EU Non Proliferation Consortium, Marzo, p. 11

STANDARD

La standardizzazione riguarda i processi di sviluppo e applicazione di standard tecnici. In UE, il sistema è costituito dalle European Standards Organisations (ESOs), vale a dire il Comité européen de normalisation (CEN), il Comité européen de normalisation en électronique et en électrotechnique (CENELEC) e lo European Telecommunications Standards Institute (ETSI). Le ESOs definiscono uno standard come un documento, approvato per consensus da stakeholder, incluse autorità pubbliche ed industrie, che partecipano su base volontaria. Lo standard che fornisce linee guida, caratteristiche e regole relative all'uso e/o qualità e risultati attesi da un materiale, prodotto, processo o servizio[134], tutti aspetti collegati con la trasferibilità di tecnologie/prodotti e processi. La CE può assegnare alle ESOs il compito di sviluppare standard[135] e circa 1/5 degli standard europei sono sviluppati su suo mandato.

L'adozione di standard così sviluppati nella maggior parte dei casi non è obbligatoria, ma resta volontaria. Una volta adottati, tuttavia, i National Standardisation Bodies (NSBs) dovrebbero trasporli in standard nazionali analoghi, ritirando eventuali standard nazionali confliggenti. L'impatto dell'adozione di standard sulle aziende varia quindi in base dell'obbligatorietà e all'effettività del regime di enforcement. In alcuni casi, gli standard europei possono diventare obbligatori in atti legislativi riguardanti *mandatory requirement*, come nel caso della previsione di *technical requirements* obbligatori, in base a specifiche previste da standard[136].

Per far fronte alla mancanza di standard europei nel settore della sicurezza, nel 2011 la CE aveva emesso un mandato su tre aree: 1) campionamento nel settore CBRN; 2) identificatori biometrici per la sicurezza delle frontiere; 3) interoperabilità nelle comunicazioni, da impiegare nella gestione delle crisi e nelle attività portate avanti dalla Protezione Civile. Tale mandato (M/487) ha dato luogo ad una approfondita riflessione sulle criticità presenti nella politica di standardizzazione dell'Unione. È seguita la pubblicazione, da parte del CEN, di diversi standard in materia di interoperabilità – come *Video-surveillance – Export interoperability* (2014)[137] – e di CBRN. Tra questi ultimi figurano, ad esempio, il *CBRN – Vulnerability Assessment and Protection of People at Risk* (2013) che, stabilendo un lessico comune, permette una condivisa comprensione degli incidenti e una comunicazione efficace, e lo *European CBRNE Glossary* (2020) che mira a fornire strumenti

[134] CEN-CENELEC, "European Standards"
[135] CE, "Standardisation policy"
[136] YourEurope (2021), "Standards in Europe"
[137] CEN (2014), "Societal security - Video-surveillance - Export interoperability (ISO 22311:2012)"

per la valutazione delle vulnerabilità a livello della popolazione[138]. Da ultimo, l'UE ha identificato nella *EU Strategy on Standardisation* del 2022 delle aree in cui lo sviluppo di standard è ritenuto strategico. Tra queste rientrano, ad esempio, il riciclaggio di materie prime critiche, la sicurezza, l'autenticità e l'affidabilità dei chip, l'interoperabilità dei dati e la loro condivisione, che saranno oggetto di mandato alle ESOs[139]. Un High-Level Forum della CE riunirà Stati membri, ESOs, comparto industriale e società civile per facilitare un confronto sulle principali necessità europee in termini di standardizzazione.

Il settore della difesa presenta un alto livello di standardizzazione e top-down, ma con diversità nazionali generalmente più marcate rispetto a quelle del settore civile/sicurezza. Gli standard sviluppati da NATO ed EDA, infatti, dovendo essere negoziati multilateralmente, hanno spesso un livello di specificità minore e richiedono ulteriori definizioni nazionali. La tradizionale esistenza di agenzie di standardizzazione militari nazionali fa sì inoltre che nonostante i processi di uniformizzazione portati avanti da NATO ed EDA significative differenze continuino a rimanere negli standard più dettagliati.

Il tema della uniformizzazione/armonizzazione tra standard è rilevante. La divergenza tra standard nazionali può impattare negativamente sulla competitività dell'industria europea e del mercato unico aumentandone la frammentarietà a livello di offerta e di domanda. Tale situazione può rappresentare una barriera nella misura in cui le aziende potrebbero essere costrette a sottoporsi a certificazioni diverse in base ai diversi standard nazionali, con costi economici e di transazione (peso amministrativo) particolarmente sentiti dalle PMI.

A livello europeo inoltre da alcuni anni si è fatta strada la possibilità di definire standard ibridi per alcuni settori. Una esperienza significativa in tal senso riguarda il settore aerospaziale europeo con comitati congiunti civili-militari per la definizione di standard ibridi. L'iniziativa coinvolge la Single European Sky ATM Research (SESAR), pilastro tecnologico del Single European Sky (SES) volto a incrementare la performance del sistema di Air Traffic Management (ATM) in Europa limitando la frammentarietà che lo caratterizza in termini di utenti sicurezza/civile e difesa. Altro ambito coinvolto per la definizione di standard ibridi è quello più prettamente spaziale, specialmente per i pilastri del programma spaziale dell'UE Galileo e Copernicus. Entrambi prevedono usi sia per attori civili/sicurezza che militari. Oltre ad avere un Open Service aperto all'utilizzo di tutti gli utenti, anche di Paesi terzi, Galileo ha uno specifico security service – il PRS ad accesso limitato/controllato e destinato a diversi utenti, militari ma anche di sicurezza tra cui: fire brigades, health services (ambulance),

[138] CEN (2013), "CBRN - Vulnerability Assessment and Protection of People at Risk"; CEN (2020), "European CBRNE glossary"
[139] CE, "Standardisation policy"

humanitarian aid, Search and Rescue (SAR), police, coastguard, border control, customs, civil protection units. Per quanto riguarda Copernicus, i servizi sono prettamente scientifici e civili, ma allo stesso tempo tutti disponibili per i militari (open services). In particolare, da evidenziare il servizio di security ed emergency a supporto ad esempio dell'EU External Action Service o di Frontex, sul quale il Crisis Management and Planning Directorate (CMPD) ha un certo livello di controllo. La definizione degli standard di utilizzo dei due programmi prevede end-users sia civili che militari e lo sviluppo del Security Accreditation Board (SAB) dell'Agenzia per il Programma Spaziale dell'UE (EUSPA) va nella direzione di un comitato congiunto per la definizione di standard potenzialmente ibridi.

CERTIFICAZIONI

La certificazione è un processo attraverso il quale una autorità esterna conferma che una tecnologia o prodotto (o una persona o una organizzazione) possiedono determinate caratteristiche (es. rispettano uno standard). Questo può essere caratterizzato da diversi aspetti come l'insieme dei soggetti cui si applica, la tipologia del processo di registrazione, i criteri imposti, i vantaggi che garantisce e soprattutto l'obbligatorietà o meno per l'azienda nel caso in cui intenda partecipare ad un determinato settore industriale o avere accesso a determinate tecnologie (trasferimento).

Non esiste una politica di certificazione a livello UE per tecnologie e prodotti di sicurezza e dual-use[140]. Questa non esiste neanche per tecnologie e prodotti militari, restando una materia di competenza nazionale. Come per gli standard, anche la compliance aziendale verso le certificazioni sconta la difficoltà legata alla scarsa armonizzazione delle policies nazionali e include per le aziende il rischio di costi aggiuntivi per la richiesta di certificazioni diverse in diversi Paesi per la stessa tecnologia, prodotto, processo. Secondo alcuni, la certificazione dovrebbe avere costi contenuti da opportune sovvenzioni al fine di non risultare un ennesimo ostacolo imposto soprattutto alle PMI o ad enti con limitate risorse anche per la comprensione di quadri regolamentari. Come la standardizzazione, la certificazione può funzionare da facilitatore per progetti di collaborazione in R&S[141]. Considerazioni su vantaggi e problematiche svolte nel paragrafo precedente a proposito di policies e normative sugli standard sono sostanzialmente replicabili in ambito policies e normative per le certificazioni.

[140] Europe Economics (2014), "Enhancing support to SMEs", p.63
[141] EDA (2014), "Your Guide to European Structural Funds for Dual-use technology projects", p.1

IPRs

La definizione di diritti di proprietà intellettuale impatta fortemente sulla possibilità di poter realizzare trasferimenti di tecnologia, anche da ambito civile/sicurezza a militare e viceversa. Esistono differenti regimi di attribuzione, accesso, uso (Ownership, Access, Use) degli IPRs. Esistono anche diverse tipologie di IPRs tra cui, in progetti di collaborazione in R&S: Background IPRs preesistenti all'inizio del progetto e Foreground IPRs generati in esecuzione del progetto (diversamente da Sideground IPRs, in cui lo sviluppo avviene durante il periodo di svolgimento del progetto, ma non in esecuzione dello stesso). La materia è complessa.

Come osservato da alcuni, se l'IPR è di proprietà della PMI richiedente, questa sarà incentivata perché in fasi successive del progetto potrebbe fare un'offerta indipendente, in partenariato con una Prime o potrebbe vendere l'IPR. Se al contrario gli IPRs restano in capo all'autorità nazionale di difesa, il richiedente è poco incentivato[142]. La posizione negoziale delle PMI, alla fine della fase di fattibilità, è tendenzialmente debole anche a causa della possibile mancanza di protezione dei brevetti nelle tecnologie di difesa e, di conseguenza, il ritorno che le PMI potrebbero aspettarsi dai propri IPRs potrebbe essere limitato[143].

Ad esempio, a livello europeo, EDA e CE non hanno uguali regimi IPRs per i progetti di R&S che finanziano: in ambito EDA (defence) gli IPRs restano in capo al finanziatore, mentre in ambito UE (civil security) sono in capo al Consorzio di ricerca. In tale contesto, ci possono essere diversi e contrastanti interessi da gestire e la situazione può variare da normativa a normativa e da contratto a contratto. Alcuni commentatori ritengono di approfondire aspetti relativi agli IPRs in attività EDA. Questi sono di due tipi: a finanziamento comune oppure a finanziamento governativo dedicato. Nel primo caso si tratta di fondi del bilancio EDA. Nel secondo caso, si tratta di fondi stanziati ad hoc dai MDIF interessati. In Italia, i finanziamenti in ambito R&T coprono solo il 50% della quota nazionale, perché la rimanente parte rimane a carico dell'industria/centro di ricerca/università interessata. Questo è fatto a similitudine di quanto in Italia si fa per le attività R&T in ambito militare: si finanzia con bilancio pubblico il 50% dell'attività, così testando il reale interesse dell'azienda interessata al finanziamento perché questa deve corrispondere una quota dell'investimento e, conservando la proprietà dei risultati, la può rivendere traendone profitto.

In fase di preparazione della PADR, la Federazione Aziende Italiane per l'Aerospazio, la Difesa e la Sicurezza (AIAD) osservava che gli IPRs sono essenziali per le industrie della

[142] Europe Economics (2014), "Enhancing support to SMEs", p.128
[143] Europe Economics (2014), "Enhancing support to SMEs", p.4

difesa a causa del loro impatto su innovazione e competitività. Di conseguenza, le regole per la gestione degli IPRs devono tenere in considerazione gli interessi sia di chi finanzia il progetto, sia di chi riceve il finanziamento. La proprietà dei risultati deve spettare all'operatore che li genera e l'operatore deve mantenere la totale proprietà dei propri background IPRs. Lo schema contrattuale suggerito considerava quanto segue: nel caso di un contratto di appalto, il cliente o i clienti devono essere definiti e i diritti di utilizzo per tale cliente devono essere la controparte del pagamento del prezzo del contratto. Nel caso di un contratto di grant, i diritti d'uso dovrebbero spettare agli operatori che svolgono la ricerca; la CE e gli Stati membri otterrebbero diritti come quelli stabiliti dall'articolo 49.2 del Regolamento UE 1290/2013 (accesso gratuito a fini non commerciali e non competitivi)[144]. L'ulteriore accesso da parte di clienti non europei ai prodotti sviluppati sulla base del programma di ricerca UE deve seguire i regolamenti europei e nazionali sulla sicurezza della difesa (licenze di esportazione, certificati di utente finale, etc.)[145]. Su questo, la PADR – attiva dal 2017 al 2019 e con investimenti su 18 diversi progetti di ricerca – ha adottato un modello simile a quello H2020: gli IPRs risultanti di proprietà dei beneficiari, con misure per informare gli Stati degli outcomes dei progetti[146].

[144] PE e Consiglio dell'UE (2013), "Regolamento (UE) N. 1290/2013 che stabilisce le norme in materia di partecipazione e diffusione nell'ambito del programma quadro di ricerca e innovazione (2014-2020) - Orizzonte 2020 e che abroga il regolamento (CE) n. 1906/2006", 11 Dicembre

[145] ASD (2015), "Technology Priorities for the EU Preparatory Action on CSDP-related research", 14 Ottobre, p. 5

[146] CE, "Preparatory Action on Defence Research (PADR)"

CAPITOLO 3 – PRINCIPALI AZIONI E APPROFONDIMENTI LATO PUBBLICO

DOMANDA

È opinione diffusa che la domanda pubblica sia centrale nell'innovazione dual-use. Si è visto come la formulazione della domanda pubblica in ambito militare sia diversa da quella civile/sicurezza, generalmente technology-oriented la prima e mission/application-oriented la seconda.

Una prima raccomandazione riguarda l'opportunità di condurre un'analisi comparata dei diversi sistemi di procurement di amministrazioni potenzialmente di interesse per sinergie dual-use. Mentre la Difesa è molto strutturata, non è lo stesso per il MINT o per le componenti operative del sistema di Protezione Civile. Questo anche in un'ottica di crescente attività delle FFAA a supporto di altri Ministeri tramite le proprie competenze e capacità[147], incluse maggiori opportunità di interoperabilità. Tale analisi deve essere condotta sulla base di un mandato istituzionale con l'avvio di Tavoli Tecnici dedicati e supportati da esperti privati anche considerando la differenza tra attività di ricerca e attività di procurement. Secondo alcuni esperti non si possono fare bandi di ricerca con il modello del procurement. I bandi di ricerca presentano peculiarità, come le fasi di test e il livello di condivisione dei rischi, che devono escludere un trattamento del tipo contratto di acquisto. Un progetto di ricerca è comprensivo, ma può fermarsi se la prima fase non dà i risultati sperati – se viene invece considerato come un acquisto di ricerca, si rischia di pagare tutto senza ottenere nulla. Si consideri, ad esempio, che ad alcuni livelli, come nel settore R&T, attualmente non risulta alcuna collaborazione tra Difesa e MINT e più precisamente non risulta che il MINT finanzi attività di R&T.

Uno degli scopi dell'analisi comparata dovrebbe essere valutare se sia possibile - in alcune aree di interesse compatibile o comune tra diversi Ministeri/Enti degli ambiti civile/sicurezza e militare - formulare una domanda pubblica basata sulle funzioni. L'individuazione delle funzioni legate alle esigenze operative è centrale per estendere la ricerca di soluzioni in settori inversi e in tal modo favorire R&S dual-use e trasferimento di tecnologie e prodotti dual-use. Alcuni commentatori assimilano entrambi i concetti nelle sole esigenze operative, ma tecnicamente si dovrebbe considerare che mentre le funzioni

[147] MDIF (2018), "Duplice uso e Resilienza. Documento di integrazione concettuale delle linee programmatiche del dicastero", p. VIII

esprimono appunto una funzionalità (es. comunicazione) le esigenze operative rappresentano i compiti da soddisfare (es. SAR).

Dal punto di vista militare, questo richiederebbe che - in alcune aree di interesse compatibile o comune tra diversi Ministeri/Enti degli ambiti civile/sicurezza e militare - la domanda si basi non su un technology-oriented approach e sulla richiesta diretta di tecnologie, ma proprio sulle esigenze operative ed in particolare sulle funzioni associate al soddisfacimento delle stesse (mission/application-oriented approach). A livello italiano, in ambito Difesa si tratta di individuare le funzioni fondamentali per assicurare un processo avente natura ciclica, con la pianificazione operativa dell'Area tecnico operativa dello Stato Maggiore della Difesa (SMD). Alcuni studi raccomandano che l'EDA incoraggi i National Armaments Directors (NADs) a non essere prescrittivi e cioè chiedere alle aziende di proporre soluzioni ai problemi piuttosto che specificare come un problema debba essere risolto[148]. I NADs, infatti, chiedono spesso tecnologie molto specifiche e questo limita la possibilità per le aziende che hanno sviluppato tecnologie per scopi civili/sicurezza e dual-use, di modificarle per soddisfare requisiti militari. Il costo dell'appalto potrebbe in tal modo anche essere contenuto in quanto i costi di R&S sarebbero già parzialmente sostenuti dall'azienda nell'ambito delle proprie attività civili/sicurezza[149]. In Italia esiste inoltre anche un'altra questione, diversa, ma collegata alla possibilità di esprimersi su "funzioni". Si tratta della modalità di funzionamento del PNRM, che prevede l'indicazione di aree tecnologiche di interesse prioritario molto vaste (es. intelligenza artificiale) su cui si accettano proposte unsolicited. Secondo alcuni, mettere a bando su funzioni almeno una parte dei fondi del PNRM, sarebbe utile alla comparazione con funzioni di altri Ministeri/enti del settore civile/sicurezza. Si tratterebbe di una eventuale operazione da condurre con misura, perché è anche vero che è proprio il carattere unsolicited del PNRM che permette un "technology watch" sul quadro complessivo nazionale dello stato della ricerca di interesse militare. La misura da trovare sarebbe comunque agevolata se venissero aumentati i fondi che restano largamente insufficienti: una media di meno di 50 milioni di euro l'annoche devono anche servire a coprire fasi successive di progetti iniziati ad essere finanziati in anni precedenti. Nel 2021, sono state finanziate meno di 30 proposte, sulle 300 arrivate, e questo dimostra sia la necessità di aumentare i fondi, sia un notevole bacino su cui condurre un simile technology watch. Sarebbe inoltre opportuno avere un budget a parte per le Emerging and Disruptive Technologies (EDTs) con un modello di call specifico che rispecchi anche una gestione del rischio diversa.

[148] Europe Economics (2014), "Enhancing support to SMEs", p.5
[149] Ivi, p.133

Tornando alle aree tecnologiche di prioritario interesse del PNRM, indicate dall'Autorità politica e condivise da SMD è da rilevare che, al fine di indirizzare maggiormente le proposte, il V Reparto ha suggerito la definizione di alcune traiettorie tecnologiche. Esse mirano a conseguire obiettivi tecnologici raggiungibili entro determinate scadenze temporali, di massima triennali, su cui andrebbero a incardinarsi le prospettive dei vari operatori nazionali del settore prescelto per l'analisi. Dette traiettorie andrebbero messe a punto in collaborazione e condivisione con altri Ministeri/Enti interessati agli specifici ambiti tecnologici, prevedendo il coinvolgimento di tutti gli attori e stakeholder competenti in materia – accademici, industriali e anche governativi – e prevedendo che gli obiettivi tecnologici della traiettoria possano attingere anche da fondi dell'EDF.

Un successivo scopo dell'analisi comparata dovrebbe essere quello di verificare la possibilità di stabilire meccanismi per individuare o definire – in alcune aree di interesse compatibile o comune tra diversi Ministeri/Enti degli ambiti civile/sicurezza e militare - esigenze operative compatibili o comuni da soddisfare e, soprattutto, funzioni associate compatibili o comuni. Ciò renderebbe possibile una comparazione sullo stesso piano, quello appunto delle funzioni[150] e favorirebbe l'individuazione di applicazioni dual-use per capacità che possano essere sviluppate in comune o trasferite - quindi in fasi a monte dei programmi R&S delle varie amministrazioni, o a valle (tecnologie e prodotti) per permettere procurement comuni – rispetto a quelle invece peculiari al solo settore civile/sicurezza o al solo militare. Questa rappresenterebbe un'impostazione utile anche ai fornitori dei settori inversi.

Dal punto di vista dell'investimento Difesa, ciò implicherebbe la considerazione di tutti i livelli di TRL raccordando le fasi technology-push con capability-pull[151]. Il coordinamento interministeriale e il collegamento con i fornitori del mercato inverso sarebbe quindi in linea con modelli di open innovation che facciano dialogare gli attori dei diversi settori civile/sicurezza e difesa, ad esempio tramite piattaforme basate su partnership pubblico/private volte a monitorare la domanda pubblica emergente per metterla in contatto diretto con la fornitura di soluzioni innovative provenienti dalla catena comprendente grandi industrie, PMI, start-up e spin-offs[152]. Sulla stessa linea si trova la *Direttiva per la politica industriale della Difesa* (2021) che tra gli obiettivi indica quello di integrare PMI nei programmi di sviluppo di capacità militari innovative per rafforzare il loro posizionamento strategico anche attraverso il ruolo dei distretti tecnologici[153]. Resta fermo che l'attuazione

[150] Ecorys (2012), "Study on Civil Military Synergies in the field of Security", Maggio
[151] MDIF (2021), "Direttiva per la politica industriale della Difesa", p.10
[152] Leonardo Company (2018), "The Italian aerospace, defence and security industry" p.31
[153] MDIF (2021), "Direttiva per la politica industriale della Difesa", p.14

di questi possibili progressi deve considerare un fattore chiave, secondo alcuni il più difficile da plasmare: la cultura pubblica e la cultura aziendale, che dovrebbero attuare un cambio di mentalità riguardo, tra l'altro, le modalità con cui la tecnologia è capita ed integrata nei sistemi[154].

Per quanto detto sopra, nelle aree in cui si rilevino funzioni compatibili o comuni dovrebbe essere verificata la possibilità di stabilire meccanismi per definire requisiti tecnici comuni/dual-use tra ambito civile/sicurezza e militare, inclusi adattamenti a requisiti espressi e formalizzati da amministrazioni centrali o locali del settore inverso.

Alcuni ritengono che questo elemento di aggregazione della domanda potrebbe essere facilitato, ad esempio, dallo sviluppo di bricks tecnologici comuni basati su tecnologia COTS con funzionalità native – ovvero sviluppate in origine con l'obiettivo di essere utilizzate su un sistema specifico – impiegabili in entrambi i comparti civile/sicurezza e militare. Altri sostengono invece che il vero tema sulle tecnologie dual-use dovrebbe invece essere proprio la convergenza di requisiti militari e civili/sicurezza che producano technology roadmaps, vale a dire strumenti della pianificazione strategica per lo sviluppo di tecnologie lungo una direzione temporale, con aggiornamenti periodici e regolari che riflettano l'evoluzione degli sviluppi nel settore. Queste roadmap dovrebbero illustrare i casi in cui la tecnologia prodotta può trovare applicazioni civili/sicurezza o militari, senza che l'una o l'altra applicazione richieda la modifica della tecnologia sottostante al punto da renderla non riconducibile allo sviluppo iniziale. È quindi una questione anche di portata dell'adattamento della tecnologia. Questa dualità applicativa sarebbe possibile solo se la technology roadmap è condivisa da entrambe le tipologie di utilizzatori finali. In tal senso anche la CE, nel suo *Piano d'azione sulle sinergie*, si impegna a sviluppare delle technology roadmap (Azione 4).

Potrebbero essere istituiti comitati congiunti per arrivare alla definizione di requisiti comuni/dual-use. In tal senso, lato militare, il livello tecnico SGD/DNA avrebbe senz'altro un ruolo nell'individuazione di standard comuni e nel coordinamento ed armonizzazione di requisiti comuni tra il settore militare e quello civile/sicurezza. In Italia, in ambito spazio, è da menzionare la conclusa esperienza di Tavoli Tecnici gestiti a livello della Presidenza del Consiglio nell'ambito della "Struttura di Coordinamento" istituita nel 2018 a supporto delle attività del Comitato interministeriale per le politiche relative allo Spazio e all'Aerospazio (COMINT). La Struttura prevedeva l'attività informativa di vari gruppi di lavoro con relativa elaborazione di documenti e veniva allargata in qualità di consulenti tecnici a rappresentanti delle associazioni di categoria, alle aziende e alle istituzioni accademiche e di ricerca. Tale

[154] Fiott, D. (2020), "Improving the Crucial Link between Civil, Defence and Space Industries: The Technology and Innovation Dimension", EU Institute for Security Studies, 5 Novembre, p. 2

meccanismo ha dato risultati molto positivi, forse in parte facilitato da un numero di attori spaziali limitato, se confrontato a quello che si avrebbe nel caso di un comitato interministeriale esteso a tutti i Ministeri potenzialmente interessati dal dual-use.

Secondo diversi esperti, anche in ambito dual-use, sulle proposte sopra descritte, sarebbe opportuna la costituzione di un Tavolo Tecnico decisionale presso la Presidenza del Consiglio dei Ministri (PCM), con un livello politico e un livello operativo con gruppi di lavoro focalizzati per tematiche (anche nel senso di selezione di iniziali settori di interesse dual-use) e gestiti con obiettivi e scadenze. I due livelli sono indispensabili entrambi per evitare che a dichiarazioni di intenti a livello strategico non faccia seguito l'esecuzione, ma anche per evitare che il livello operativo, lasciato senza guida politica finisca per non individuare ed attuare obiettivi. Una soluzione meno neutra sarebbe rappresentata dal Tavolo Tecnico di coordinamento della Politica Industriale (TTPI) presso il MDIF, previsto dalla *Direttiva per la politica industriale della Difesa* (2021). Ci si aspetta dal TTPI un ruolo centrale, avendo tra i suoi compiti quello del raccordo con gli altri Ministeri[155]. Il costituendo TTPI avrà un livello politico, presieduto dal Ministro della Difesa ed uno tecnico presieduto dal SGD/DNA.

I possibili interventi sopra esposti implicano un coordinamento interministeriale in linea con la *Direttiva* che nomina in maniera specifica la necessità di collaborazione tra MDIF, MUR, MIMS e MiSE a livello governativo e con CNR, Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (ENEA) e ASI a livello di enti di ricerca, oltre ai livelli accademico, scientifico ed industriale[156]. Questo coordinamento deve far emergere un Sistema Difesa che innovi il rapporto Difesa-industria coinvolgendo anche altre componenti nazionali, così mostrando anche all'opinione pubblica il passaggio da una Difesa "costo" ad una Difesa "valore"[157]. In realtà, in Italia le FFAA hanno tradizionalmente significativi ruoli di immediato impatto positivo sui cittadini, ma deve essere impostata una valida strategia di comunicazione. Una Difesa che sia presidio di sovranità tecnologica, crescita economica e di occupazione, anche in un'ottica di controllo degli investimenti esteri, ma soprattutto di coerenza, stabilità e qualità degli investimenti nazionali rafforzata da maggiori sinergie tra la Difesa e le industrie civili[158].

Anche raccomandazioni istituzionali a livello europeo si muovono in questa direzione, ad esempio riguardo incontri regolari tra Comitati dei programmi di sicurezza e comitati dei

[155] MDIF (2021), "Direttiva per la politica industriale della Difesa", p.17
[156] Ivi, p. 7
[157] Ivi, p. 6
[158] MDIF (2021), "Direttiva per la politica industriale della Difesa", p.4

programmi difesa per scambi su bisogni e requisiti su aree di possibile interesse comune[159]. La corrispondenza temporale tra definizione ed espressione della domanda pubblica dei diversi settori civile/sicurezza e militare resta comunque una condizione di problematica realizzazione. Si tratta infatti di due archi temporali generalmente diversi: militare su pianificazione anche pluriennale, civile/sicurezza secondo necessità, anche se con un minimo di pianificazione per il settore governativo. Minore dovrebbe essere il peso della corrispondenza temporale nel caso di prodotti già sviluppati. Restano comunque caratteristiche differenti tra i due settori, tra cui requisiti che in ambito difesa entrano in gioco in fasi iniziali della R&S rispetto a quelli della sicurezza, come anche il fatto che la ricerca in ambito difesa è generalmente guidata da un approccio predittivo e da necessità di capacità di più lungo termine rispetto all'ambito sicurezza, in cui l'approccio è più reattivo e con proiezione di medio termine[160].

In tale contesto gli standard devono essere tenuti in considerazione. In particolare, gli standard inseriti in requisiti tecnici che caratterizzano tecnologie e prodotti per i diversi settori civile/sicurezza o militare. La dualità è inversamente proporzionale alla curva della standardizzazione che caratterizza tecnologie e prodotti verso un contesto di applicazione definito civile/sicurezza o militare. La possibilità di R&S dual-use e/o trasferimento di tecnologie e prodotti dual-use resta direttamente proporzionale alla compatibilità tra standard dei diversi ambiti e alla possibilità di standard ibridi.

Come noto, i processi di standardizzazione sono lunghi e possono durare anche anni. Da tempo si registrano iniziative istituzionali europee volte alla creazione di standard ibridi, come ad esempio nella Comunicazione della CE *Verso un settore della difesa e della sicurezza più concorrenziale ed efficiente*[161]. Con il mandato M/487, nel 2012, la CE aveva emesso una richiesta di standardizzazione per standard ibridi in materia di Software Defined Radio (SDR), ribadendo inoltre il bisogno di svilupparne su rilevamento e campionamento di eventi CBRN, RPAS, requisiti di aeronavigabilità, data sharing, crittografia ed altre tecnologie di informazione e comunicazione critiche[162]. Secondo alcuni esperti, standard ibridi per l'applicazione sono necessari soprattutto in ambito di interoperabilità e comunicazione. Anche nell'EDAP, la CE faceva riferimento alla creazione di standard ibridi in accordo con EDA e Stati membri, in particolare al fine di progetti di cooperazione in aree prioritarie. L'EDA dal 2015 ha stabilito una procedura per l'elaborazione di standard ibridi che prevede un meccanismo di consultazione interna tra EDA, CE e Defence

[159] PASAG (2020), "Optimising access to dual-use R&T and R&D results for security", CE, p.7
[160] Ivi, p.10
[161] CE (2013), "Verso un settore della difesa e della sicurezza più concorrenziale ed efficiente", 24 Luglio
[162] CE (2012), "Mandate addressed to Cen, Cenelec and Etsi for Reconfigurable Radio Systems M512"

Standardisation Cooperation Group (DSCG) delle ESOs[163]. L'EDA si è fatta inoltre promotrice dell'applicazione di standard civili al settore della difesa che, secondo l'Agenzia, potrebbe garantire un risparmio stimato tra il 10% e il 50%. In tale contesto, e in collaborazione con CEN e CENELEC, l'EDA ha realizzato lo European Defence Standards Reference System (EDSTAR), un database che raggruppa gli standard applicabili ai fini della difesa, e in cui figurano diversi standard provenienti dal settore civile.

Da ultimo, nel *Piano d'azione sulle sinergie* si stabilisce che la CE, insieme agli stakeholder di rilievo, presenterà entro la fine del 2022 un Piano per promuovere l'uso degli standard ibridi esistenti e lo sviluppo di nuovi (Azione 5)[164]. Tra gli esempi di settore, il Piano riporta CBRN a livello di utenti (agenzie di protezione civile) e a livello industriale, i dati in materia di sicurezza, nel contesto del programma Europa Digitale[165]. Nella recente *EU Strategy on Standardisation* (2022) la CE richiama il Piano riguardo gli standard ibridi e si pone l'obiettivo di assumere la leadership a livello internazionale nell'elaborazione di standard in ambito civile. Ciò dovrebbe essere utile anche per il settore difesa, dal momento che quasi l'80% delle norme utilizzate in difesa provengono dal settore civile[166].

Diversi rappresentanti industriali e della Difesa concordano sul potenziale della definizione di standard ibridi per una maggiore aggregazione della domanda (e dell'offerta) nel mercato dual-use di intersezione tra i mercati civile/sicurezza e difesa. Altri esperti sottolineano come gli standard ibridi siano fondamentali specialmente per le PMI, per le quali, ad esempio, chiedere l'accesso a standard NATO implica un processo lungo, a differenza delle grandi aziende che già sono informate. Lo standard ibrido dovrebbe invece essere di più facile accesso. Senza standard ibridi si avrebbe un problema di costruzione della tecnologia stessa e di trasferimento degli IPRs. La possibilità di standard ibridi resta comunque da analizzare caso per caso, sia a livello di fattibilità che a livello di opportunità, a seconda della natura di tecnologie e prodotti. Alcuni osservano che il concetto di standard ibrido sembrerebbe burocratico, più volto a una visione di mercato che di impiego. Impiego che è caratterizzato da differenti ambienti di utilizzo, differenti skill degli end-user e differenti regole d'ingaggio. Gli standard ibridi rispondono comunque a necessità come quelle determinate dall'assenza di riconoscimento reciproco tra standard di sicurezza e di difesa che implica, per l'utilizzo di una tecnologia, prodotto o componente, il ricorso ad un nuovo e diverso procedimento di certificazione valido per l'ambito inverso. Questo soprattutto in ambito militare, perché invece in altri settori non è detto che si certifichi la compliance con

[163] EDA, "European Defence Standardisation"
[164] CE (2021), "Piano d'azione sulle sinergie", p.12
[165] Ibid.
[166] CE (2022), "Tabella di marcia relativa alle tecnologie critiche per la sicurezza e la difesa", p.14

uno standard. Secondo altri, in linea teorica, una volta accettati gli standard ibridi rendono più facile l'applicazione – ovvero sono necessari, ma non sufficienti - ma ad ogni modo rappresentano anche un tassello del processo di avvicinamento culturale tra i due ambiti sicurezza/civile e militare. Resta la difficoltà riscontrata in questi anni per definire standard ibridi e il dato che il carattere volontario sull'adozione degli stessi ne rende meno prevedibile il reale effetto.

CAUTELE PER LA DIFESA

Nel valutare l'innovazione dual-use, la Difesa deve garantire la propria funzionalità e le proprie peculiarità cercando il giusto punto di equilibrio perché, dal punto di vista del cliente militare, il dual-use può comportare pro e contro.

La ricerca di esigenze operative, funzioni e requisiti compatibili, comuni, dual-use non deve arrivare ad una forzata convergenza che potrebbe comportare riduzioni di capacità (nella parte alta del requisito) o loro eccessi (nella parte bassa), ad esempio nel settore della mobilità. Soprattutto negli impieghi più operativi, i compromessi tra prestazioni (grado di corrispondenza ai requisiti) e costi (di sviluppo, ricorrenti) devono evitare il rischio di rapporti costo-efficacia negativi, ma soprattutto di mancato riconoscimento delle esigenze specifiche della Difesa o riduzione delle capacità esprimibili, altrimenti il ritorno è negativo.

Un altro problema è costituito dalla difficoltà nel tracciare origine/proprietà/design authority delle tecnologie commerciali e nel valutare l'autonomia/dipendenza connessa all'impiego di queste (problemi di sicurezza, dipendenza tecnologica). Sul possibile aumento di dipendenza da tecnologie straniere[167] e commerciali è da considerare che comunque l'autonomia completa non esiste: la dipendenza non è evitabile, è solo mitigabile, ad esempio basandosi su più fornitori. La natura dual-use potrebbe in alcuni casi diventare un problema se l'industria che sviluppa la tecnologia decide di farla evolvere seguendo gli input del mercato civile. Per fare un esempio teorico, se una azienda del tipo Apple usa una crittografia dual-use per vendere brani musicali e, in teoria, vende la stessa al Department of Defense (DoD) statunitense, dopo dieci anni farà evolvere la tecnologia seguendo i bisogni del DoD o quelli di 200 milioni di utenti nel mondo? Probabilmente seguirà il ritorno su investimenti con gli effetti negativi che ne conseguono per il cliente Difesa. Come osservato da alcuni autori, le argomentazioni economiche perfettamente razionali per le tecnologie dual-use non dovrebbero portare le imprese a stabilire condizioni di produzione senza il dovuto riguardo per le esigenze strategiche. Alcuni sostengono, infatti, che l'enfasi

[167] Cappelletti, G. M. (2015), "The European Structural and Investiment Funds (ESIFs) e il settore della Difesa", Centro Alti Studi per la Difesa, 6 Ottobre, p.14

sulle tecnologie dual-use potrebbe ulteriormente "civilizzare" il settore della difesa in Europa concedendo agli operatori commerciali la precedenza sui militari[168].

Quali correttivi potrebbero essere adottati dalla Difesa?

Un possibile suggerimento è quello di attuare, ed aggiornare una selezione di aree (esigenze operative e funzioni) in cui il dual-use sia realizzabile senza compromissione della funzionalità dello strumento militare, escludendo quindi quelle puramente militari e mantenendo due linee di investimento separate: military only e dual-use[169]. Una scelta più politico-strategica che tecnico-operativa. Anche secondo alcuni esperti industriali, in un contesto di spinta al dual-use e alle sinergie, resta opportuno mantenere una giusta misura che necessariamente preveda anche temi specifici della sola difesa (oltre a tecnologie trasversali, come quelle digitali), considerando da una parte che gli investimenti nella difesa devono poter crescere anche in termini di capability specifiche e dall'altra che, su alcuni aspetti, la difesa è molto più avanti del civile.

La maggior parte degli esperti ritiene che la definizione di esigenze operative e funzioni compatibili o comuni sia possibile solo in alcune aree operative, ad esempio in ambito law enforcement e controllo del territorio in particolare a livello di equipaggiamenti e sensoristica e, in parte, nel peace-keeping, dove i settori civile/sicurezza e militare operano a stretto contatto, ad esempio in ambito sistemi di sorveglianza. La gestione della minaccia asimmetrica e il terrorismo in ambiente urbano costituiscono un altro esempio. Ma anche Protezione Civile e la gestione di eventi CBRN. La ricerca di interoperabilità civile/sicurezza-militare può, come visto, favorire la definizione di esigenze operative comuni ai diversi settori e, conseguentemente, una domanda comune di soddisfacimento delle funzioni associate a tali esigenze operative.

Quanto ai requisiti tecnici comuni/dual-use, questi dovrebbero restare possibili per applicazioni high end civili/sicurezza e low end militari[170]. Il potenziale dual-use può passare attraverso la riduzione della parte specifica del requisito tecnico espresso da ciascun ambito civile/sicurezza e militare e attraverso la ricerca di technology bricks/basi tecnologiche comuni ai due ambiti. Questo può essere valido in alcuni casi e non in altri per non rischiare, come visto, l'abbassamento delle perfomances militari. Alcuni consigliano, ove possibile, di prevedere i cosiddetti requisiti "add-on" per i soli sistemi militari (dedicati a specifiche attività militari). È questo il caso degli Unmanned Ground Vehicle (UGV) armati (militare) e non

[168] Fiott, D. (2015), "Dual-use technologies don't justify decreasing defence budgets in Friends of Europe", September
[169] Cappelletti, G. M. (2015), "The European Structural and Investiment Funds (ESIFs) e il settore della Difesa", p.15
[170] Ecorys (2012), "Study on Civil Military Synergies in the field of Security"

armati (civile/sicurezza) dotati, però, degli stessi sistemi di rilevazione ottica e della stessa endurance/range.

CONOSCENZA TECNOLOGIA

La conoscenza di tecnologie e prodotti disponibili o in via di sviluppo e potenziali applicazioni è riconosciuto come uno dei fattori più positivi per R&S dual-use e/o trasferimento di tecnologie e prodotti dual-use. Non sempre, infatti, il potenziale ricevente di tecnologia, che ha chiaro il proprio bisogno di mercato, riesce ad interpretare il potenziale applicativo anche dal settore inverso; d'altro canto, l'owner della tecnologia non sempre ne intuisce il potenziale applicativo in settori a cui non è abituato.

La possibilità di realizzare tale conoscenza varia a seconda delle specifiche di tecnologie e prodotti ed in ambito militare trova un limite anche nella riservatezza delle informazioni. Il MDIF, nel passaggio che individua le priorità capacitive e tecnologiche e lo sviluppo e trasferimento tecnologico dedicato a soddisfare tali priorità, prevede delle attività di monitoraggio tecnologico con MUR, MiSE e CNR. Tale monitoraggio è utile per esprimere la propria funzione di indirizzo e coordinamento attraverso il PNRM. A livello internazionale, il MDIF si coordina invece con la NATO Science and Technology Organization (STO), l'EDA, la Letter of Intent-Framework Agreement (LoI-FA), lo European Technology Acquisition Programme (ETAP) e l'Organisation Conjointe de Coopération en matière d'Armement (OCCAR).

Aziende, consorzi, associazioni di categoria dovrebbero sviluppare tale conoscenza, come forma d'investimento per il proprio sviluppo sia dal punto di vista produttivo che esportativo. Questo anche nella relazione tra grandi integratori di sistemi, inclusi quelli dei settori inversi, e PMI fornitrici di tecnologia anche a bassi livelli di TRL, ma con potenziale di applicazione futura[171]. È importante evitare che, lato offerta, tale conoscenza resti basata sulla capacità divulgativa del singolo. Soprattutto in ottica di scouting internazionale, infatti, tale conoscenza può essere, secondo alcuni, portata avanti con risorse interne solo da grandi aziende/gruppi e resta di difficile praticabilità per le PMI.

Il settore pubblico dovrebbe individuare gli strumenti che possano favorire la conoscenza di tecnologie e prodotti disponibili o in via di sviluppo e potenziali applicazioni dei diversi settori civile/sicurezza e militare dunque l'incontro tra domanda e offerta anche tra settori inversi. Di seguito se ne approfondiscono alcuni: strutture di technology brokering esterne alle aziende, cluster tecnologici/industriali, database industriale europeo dual-use e

[171] Becker, H. (2015), "Three ways to support SMEs' contribution to European research in Security and Defence", Friends of Europe, p.26

database industriale europeo sulle tecnologie critiche. Ci si interroga su quali siano i migliori per monitorare l'innovazione tecnologica che si sviluppa nel quadro dual-use, al fine di individuare quanto potrebbe essere di interesse della Difesa. Secondo alcuni, questo dovrebbe includere anche il ricorso sistematico a società esterne impegnate nello scouting tecnologico (anche sul mercato internazionale) al fine di supportare gli organismi della Difesa in quest'attività. Secondo esperti istituzionali, invece, tale possibilità presenta invece almeno due ordini di problemi. In primis la garanzia di indipendenza, cioè come assicurare la corretta ed indipendente interpretazione di interesse nazionale e della Difesa da parte di società esterne private (in tal senso, per quanto riguarda il tema delle tecnologie sovrane, non può risultare ammissibile il ricorso a società terze). Infine, il problema dei costi del servizio.

TECHNOLOGY BROKERING OFFICE ESTERNO

Strutture associate alle funzioni di technology brokering office esterni alle aziende possono avere un ruolo rilevante per la R&S dual-use e/o trasferimento di tecnologie e prodotti dual-use favorendo la loro commercializzazione a clienti del mercato inverso.

È opportuno chiedersi quali siano le esperienze di maggior successo in ottica dual-use e/o quali le caratteristiche vincenti per obiettivi e modalità di funzionamento. Questa attività potrebbe essere svolta anche da imprese di ingegneria multidisciplinari o strutture accademiche/scientifiche integrate[172]. Alcuni riportano che le attività di brokeraggio istituzionale nel settore spaziale sarebbero più avanzate anche grazie a minori vincoli rispetto all'ambito della difesa. Le agenzie spaziali sono attive nell'area del technology transfer, anche a livello europeo, in cui l'ESA ha i suoi Business Incubation Centres e anche il Technology Broker Network, all'interno dell'area generale dedicata al Business Development. Nel settore spaziale, a parte l'upstream e quindi la manifattura, crescente importanza acquisisce inoltre il downstream, quindi tutto quello che gira intorno al dato spaziale/satellitare che in quanto tale può circolare maggiormente e servire più utenti e applicazioni**.**

Tali strutture possono essere sia private che sostenute a livello istituzionale, oppure in partnership pubblico-private. Un aspetto rielevante secondo alcuni è il grado di neutralità. L'ESA sembra garantirlo e, sulla stessa linea, in ambito militare, altri ritengono che sarebbe preferibile che tale attività fosse svolta da agenzie quali l'EDA. A livello europeo, infatti, alcuni esperti istituzionali ritengono che sarebbe sensato avere una struttura per il

[172] Nones, M. (2019), "L'innovazione tecnologica nei settori civile e militare", p.151

trasferimento tecnologico che faccia da driver (anche per le PMI, che non possono permettersi un'analisi di tutti gli aspetti da considerare). Esistono alcuni esempi, eterogenei e dai limitati risultati, di strutture a livello nazionale, ma sembra più efficace svolgere la cosa a livello europeo per avere maggiore massa critica. Ad una struttura di tal tipo, che può essere realizzata con più modelli (es. joint undertaking 50% UE e 50% industria), serve supporto governativo anche dal punto di vista degli investimenti, ma soprattutto supporto da parte delle aziende, dai centri di ricerca e dalle università che creano tecnologie e che devono essere facilitate nella partecipazione. Tale struttura dovrebbe anche considerare la possibilità di forme strutturate di passaggio di competenze e di skills, ad esempio sul modello di centri militari di conoscenza.

Alcuni suggeriscono la creazione di technology brokering office istituzionali trasversali alle aziende italiane operanti in ambito difesa che ricevono investimenti pubblici di R&S sia italiani che europei. Ciò consentirebbe di accedere alle informazioni in modo condiviso e permetterebbe l'applicazione ed il riutilizzo dei risultati conseguiti evitando di rifinanziare gli stessi sviluppi. Altri sostengono che, però, si potrebbe correre il rischio di appesantire il sistema della ricerca tecnologica e di non poter garantire un intervento flessibile e sempre tempestivamente aggiornato.

Alcuni sostengono che technology brokering office esterni alle aziende offrano una visione più larga di quella, magari maggiormente dettagliata, di technology brokering office interni alle aziende. Altri ritengono che gli esterni non abbiano una sufficiente conoscenza specifica verticale dei meccanismi produttivi e delle dinamiche organizzative dell'azienda e potrebbero risultare dunque meno efficaci. Secondo alcuni inoltre in caso di utilizzo di technology brokering office esterni all'azienda potrebbe sussistere un rischio di mancanza di paternità della tecnologia e conseguentemente di minore responsabilità verso l'utente finale. Probabilmente i due approcci andrebbero combinati con relazioni funzionali stabili tra technology brokering office esterni di brokeraggio istituzionale o privato e technology brokering office interni alle aziende.

CLUSTER TECNOLOGICI/INDUSTRIALI

Cluster tecnologici/industriali, di iniziativa privata o governativa, potrebbero migliorare lo scambio di informazioni tra il settore civile/sicurezza e militare, sia lato domanda che offerta, e quindi favorire R&S dual-use e/o trasferimento di tecnologie e prodotti dual-use. Anche a livello europeo, i cluster possono essere considerati uno strumento per le aziende

per sviluppare tecnologie e prodotti dual-use e/o diversificare verso nuovi prodotti/mercati[173].

È opportuno chiedersi quali siano le esperienze di maggior successo in ottica dual-use e/o quali le caratteristiche vincenti rispetto ad obiettivi e modalità di funzionamento. Non esiste infatti una definizione standardizzata di cluster. In linea generale, i servizi forniti dai cluster si possono raggruppare in tre macro-categorie non esaustive: accesso all'informazione; accesso a finanziamenti; accesso ai mercati. Per quanto riguarda l'accesso ai mercati, i cluster possono, ad esempio, supportare il collegamento tra aziende e clienti e fornire consulenza per gare di appalto, ma anche creare database su tecnologie[174]. L'adesione ai cluster sembra particolarmente interessante per PMI, in generale dotate di mezzi minori.

Il MUR li definisce come "reti di soggetti pubblici e privati che operano sul territorio nazionale in settori quali la ricerca industriale, la formazione e il trasferimento tecnologico. Funzionano da catalizzatori di risorse per rispondere alle esigenze del territorio e del mercato, coordinare e rafforzare il collegamento tra il mondo della ricerca e quello delle imprese"[175]. La composizione degli enti che costituiscono un cluster è varia e può comprendere imprese, università, istituzioni pubbliche o private di ricerca, finanziatori dell'innovazione, inclusi i Distretti Tecnologici già esistenti.

Nel 2012, il Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) ha stabilito i CTN, infrastrutture intermedie di soft-governance che facilitano il raggiungimento di obiettivi di coordinamento pubblico-pubblico e pubblico-privato. I primi 8 cluster promossi sono: Aerospazio, Agrifood, Chimica verde, Fabbrica intelligente, Mezzi e sistemi per la mobilità di superficie terrestre e marina, Scienze della Vita, Tecnologie per gli ambienti di vita, Tecnologie per le Smart Communities. Agli 8 CTN, il successivo Programma nazionale per la ricerca (PNR) 2021-2027 affianca 4 nuovi cluster: Tecnologie per il Patrimonio Culturale, Design, Creatività e Made in Italy, Economia del Mare, Energia. Ai CTN è affidato il compito di elaborare piani strategici e roadmap tecnologiche condivise su scala nazionale, tra sistemi regionali, governo centrale e imprese che costituiscano la base per strutturare e specializzare gli interventi di indirizzo e sostegno alla ricerca applicata[176]. In tale contesto è considerato un apporto specifico del MiSE che nel PNR 2015-20 era incaricato di coordinarsi con il MIUR per la creazione di matching fund per imprese, università e istituti di ricerca per

[173] Intervento (2014) durante il Workshop "Strengthening Europe's Defence Industry: Dual use and Smart Clustering", EDA, CE e European Association of Development Agencies (EURADA), Bruxelles, 25 Novembre
[174] Europe Economics (2014), "Enhancing support to SMEs", p.2
[175] MUR, "Cluster tecnologici nazionali"
[176] MUR, "Programma Nazionale per la Ricerca 2015-2020", p. 61

la partecipazione a bandi europei e ottenere risorse per progetti di ricerca industriale e di sviluppo sperimentale nei 12 ambiti di interesse individuati dalle roadmap tecnologiche dei CTN. Un ruolo, quindi, di sostegno alle imprese, anche in materia di brevetti nella valorizzazione dei fondi europei[177]. Nel PNR 2021-2027, il riferimento al MiSE risulta più limitato e indirizzato ad aree specifiche come l'Intelligenza Artificiale. Da ultimo, un ruolo attivo di finanziatori pubblici e privati, nonché la capacità di inserire le realtà dei cluster esistenti nell'ambito del Next Generation EU, sottolinea l'importanza potenziale anche nel contesto italiano di attori come Cassa Depositi e Prestiti e Primo Space, così come del Piano Nazionale di Ripresa e Resilienza (PNRR). Il PNRR, infatti, presenta occasioni importanti per lavorare anche nella direzione dei cluster e delle associazioni volte a garantire l'accesso e la partecipazione a più livelli delle realtà del tessuto industriale e di ricerca italiano.

Di particolare rilievo risulta essere il Cluster Tecnologico Nazionale Aerospazio (CTNA) relativo a "tutti gli ambiti tecnologici di rilievo per il settore aeronautico e spaziale con particolare riferimento all'uso dual-use delle tecnologie che ne specializzino l'uso ad applicazioni in campo civile e di elevato impatto sociale"[178]. Il PNR 2021-2027, infatti, identifica l'aerospazio come settore a chiare connotazioni dual-use in cui è particolarmente indicata l'ottimizzazione di obiettivi, infrastrutture, sistemi e finanziamenti. Il CTNA raggruppa tra i soci due attori industriali (Leonardo ed Avio), l'ASI, l'AIAD, il CNR, il Centro Italiano Ricerche Aerospaziali (CIRA), oltre a dodici distretti tecnologici territoriali. A livello regionale, i distretti a supporto del cluster provengono da Basilicata, Campania, Sardegna, Abruzzo, Umbria, Lazio, Toscana, Liguria, Emilia Romagna, Piemonte, Lombardia. Così come manca una definizione standard di cluster, anche i distretti non sono identificati univocamente. Si può comunque ritenere che abbiano una vocazione più prettamente tecnologico-industriale, mentre i cluster mantengono la qualità di aggregatori di attori diversi, ivi compresi i centri di ricerca, e possono focalizzarsi su obiettivi a più ampio spettro.

Un recente esempio di iniziativa privata è rappresentato dal cluster tecnologico, industriale e istituzionale per la Preparazione, Prevenzione e Protezione della popolazione e dell'ambiente dai rischi Chimici, Biologici, Radiologici e Nucleari (Cluster CBRN-P3). Un network italiano che coinvolge attori istituzionali, industriali e del mondo scientifico attivi nel campo della prevenzione e protezione della popolazione e dell'ambiente dai rischi CBRN. Nato nel 2017 su iniziativa dell'Istituto Affari Internazionali (IAI), si pone l'obiettivo di essere interlocutore credibile delle istituzioni centrali competenti per materia nonché delle istituzioni

[177] Si veda: MiSE, Ufficio Italiano Brevetti e Marchi (UIBM); MiSE, Fondo per la crescita sostenibile; MUR, "Programma Nazionale per la Ricerca 2021-2027"
[178] MUR, "Programma Nazionale per la Ricerca 2021-2027"

territoriali maggiormente interessate; di favorire la partecipazione dei suoi membri a programmi e finanziamenti europei; di favorire una maggiore attenzione dell'opinione pubblica e del mondo politico per il settore CBRN e, quindi, una crescita del settore e del mercato della protezione, della prevenzione e della gestione di eventuali emergenze del settore.

A livello italiano, ci si interroga sull'opportunità di creare un cluster nazionale dual-use e con quali caratteristiche – se riconosciuto dal MUR, privato, o di altra tipologia – e con quali mandati relativi al trasferimento tecnologico su una selezione di aree di interesse. Secondo gli esperti, il focus deve essere sul trasferimento tecnologico. Secondo altri, un Cluster sul dual-use sarebbe molto vasto da gestire e resterebbe comunque opportuna e complementare anche la trattazione di tematiche dual-use all'interno dei Cluster esistenti come avviene nel Cluster Tecnologico Nazionale Aerospazio (CTNA).

Per quanto riguarda i cluster con finalità dual-use si riporta l'esperienza del Regno Unito che nel 2015 ha creato il Dual-Use Technology Exploitation Cluster, un progetto finanziato dal Governo con oltre 10 milioni di sterline in partnership con il fondo Advanced Manufacturing Supply Chain Initiative (AMSCI). Terminato nel 2019, ha raggruppato PMI, attori industriali e università per facilitare l'identificazione e lo sfruttamento delle innovazioni tecnologiche con applicazioni dual-use. Altri esempi nazionali europei riguardano il Dual Use Cluster (DUC) in Romania e il Center for Defence, Space and Security (CenSec) in Danimarca. Il DUC romeno si identifica come organizzazione no-profit e non governativa che coinvolge attori industriali e universitari impegnati su diversi settori, anche nel tessile, nelle biotecnologie e in generale nel settore sanitario oltre che in quelli più vicini ai temi di sicurezza e difesa. Il CenSec danese ha ottenuto un riconoscimento formale come cluster da parte del Ministero dell'Istruzione nel 2020, raccogliendo gli stakeholder più vicini a difesa, sicurezza e spazio e mantenendo tra i membri università e centri di ricerca rilevanti per i temi del cluster, compreso DTU Space - National Space Institute, che agisce come un'agenzia spaziale nazionale. Il CenSec gestisce diversi progetti, di durata anche limitata a pochi mesi, che vedono coinvolti a geometrie variabili i membri del cluster insieme a "business partners", interni o anche esterni al cluster stesso, come possono essere gli stakeholder locali di progetti specifici. I finanziamenti provengono anche dalla Danish Agency for Higher Education and Science, creata nel 2020 e braccio operativo di procurement sulla ricerca del Ministero dell'Istruzione.

Oltre l'orizzonte europeo, il contesto nordamericano (Stati Uniti e Canada) presenta un pattern più marcato sulle associazioni industriali, con attività di business training, guidance e, non ultimo, di lobbying sulle istituzioni locali/regionali/statali, anche in chiave

legislativa. La realtà nordamericana presenta caratteristiche strutturalmente diverse da quelle europee ed italiane, basandosi su un contesto più abituato alle attività di lobbying e con una vocazione industriale prominente. Tali caratteristiche possono ugualmente essere di esempio per le direttrici di azione dei cluster italiani.

DATABASE INDUSTRIALE EUROPEO DUAL-USE

Alcuni studi raccomandano la definizione di un database industriale europeo relativo a tecnologie e prodotti dual-use disponibili e progetti di R&S dual-use a livello degli Stati membri e a livello UE, condiviso tra gli ambiti civile/sicurezza e militare[179]. Un simile database, volto a facilitare l'incontro di domanda e offerta, potrebbe infatti diminuire le barriere tra i mercati civile/sicurezza e militare, permettendo di valutare al meglio gli investimenti in R&S e riducendo inutili duplicazioni. Nell'avviare un'iniziativa europea che coinvolga sia istituzioni europee che Stati membri, la CE dovrebbe tener conto di best practice e lessons learned degli Stati che abbiano avviato un simile esercizio.

La definizione di un database industriale europeo è ritenuta tanto positiva quanto di difficile realizzazione: da un punto vista politico, si pone un problema di costruire un database sufficientemente aperto e pertanto realmente efficace; da un punto di vista tecnico, la necessità di continuo aggiornamento dovuto alla velocità dell'innovazione tecnologica, per l'effettiva utilità dei dati, rappresenta una complicazione ed un costo.

A livello europeo esistono strumenti per il monitoraggio tecnologico, ma non sempre le aziende ne sono a conoscenza. Ad esempio, è operativa la Enterprise Europe Network (EEN), la più estesa rete al mondo di sostegno gratuito alle PMI. Il network, co-finanziato dall'UE, supporta aziende europee in attività di innovazione e trasferimento tecnologico, affinché esse incrementino la propria competitività e crescano su scala internazionale[180]. La rete riunisce oltre 3.000 esperti provenienti da 600 organizzazioni basate in 60 diversi Paesi del mondo ed è organizzata in 6 consorzi multi-regionali[181].

Anche l'EDA ricopre un ruolo di rilievo nel monitoraggio tecnologico. Dal 2015, l'Agenzia è impegnata in attività di Technology Watch & Technology Foresight per l'identificazione di tecnologie emergenti e la valutazione del loro impatto nel lungo periodo[182]. Tali attività sono poi confluite, nel 2018, nella Overarching Strategic Research Agenda (OSRA) finalizzata alla definizione delle priorità EDA in termini di attività di ricerca

[179] Ecorys (2012), "Study on Civil Military Synergies in the field of Security", p.20
[180] Si veda: Enterprise Europe Network, "I nostri Servizi"
[181] Enterprise Europe Network, "La rete Enterprise Europe Network"
[182] EDA, "Technology Watch & Foresight"

e rispettive strategie mirate alla conduzione delle stesse[183]. A tal fine, l'OSRA ha delineato oltre 130 Technology Building Blocks (TBBs) molti dei quali riguardano tecnologie intrinsecamente dual-use – tra cui realtà immersiva, virtuale e aumentata, intelligenza artificiale, Big Data, e materiali ad alta temperatura[184]. Un meccanismo opportuno deve permettere di categorizzare tecnologie come dual-use e valutare le condizioni di trasferimento tramite il confronto con altri database presso enti non-EDA, come la CE. Tra le condizioni al trasferimento rientrano diversi aspetti, tra cui anche la presenza di standard, di limitazioni all'utilizzo e la disponibilità di eventuali funding scheme a supporto.

DATABASE INDUSTRIALE EUROPEO SULLE TECNOLOGIE CRITICHE

Alcuni, già in passato, hanno specificato l'idea di un database industriale europeo dual-use come basato sulle KETs per prospettive di progressi tecnologici e di stimolo all'innovazione non solo per applicazioni civili, ma potenzialmente anche per quelle dual-use[185]. Esso permetterebbe di monitorare quante e quali tipologie di azienda (se civili/sicurezza o militari) convergono sullo sviluppo di determinate KETs categorizzate nel database al fine di potere fornire ad un'azienda la possibilità di acquisire direttamente una KET, evitando di svilupparla oppure chiedere di unirsi al progetto di R&S se in corso, per favorire – in maniera sinergica tra più companies sia civili/sicurezza che militari che convergono nel processo di innovazione perché hanno competenze su una determinata KET – un progresso più veloce del livello di TRL per quella determinata KET.

La definizione di un database industriale europeo dual-use basato sulle KETs presenta positività e difficoltà di realizzazione simili a quelle espresse nel precedente paragrafo e, così come per il database industriale europeo dual-use, presenta rischi relativi alla possibile non univoca interpretazione di termini e contenuti.

L'importanza del dual-use nelle KETs è stata formalmente riconosciuta come scopo dell'esperienza dell'High Level Group (HLG) on KETs (2010-2011) e del suo HLG-KET Working Group on accelerating dual-use potential of KETs (2013-2014). Questo era volto a promuovere KETs con applicazioni dual-use (non solo materiali e componenti, ma anche architetture di sistema) e a studiare possibilità e modalità per combinare varie fonti di finanziamento pubblico in R&S sia a livello UE (come H2020 e ESIFs) che a livello degli Stati membri e dell'EDA (con riguardo a R&S per la difesa). Esso era inoltre volto ad

[183] EDA (2019), "Overarching Strategic Research Agenda (OSRA)", 25 Marzo
[184] EDA, "Osra Technology Building Blocks"
[185] CE (2013), "Verso un settore della difesa e della sicurezza più concorrenziale ed efficiente", p.11

identificare aree per attrarre investimenti privati aggiuntivi su una lista di tecnologie con applicazioni potenzialmente dual-use basata su identificazione di gap prioritari.

Il progetto europeo Advanced Technologies for Industry (ATI) rappresenta un passo avanti. L'ATI fornisce ai membri dell'Unione dati statistici sulla creazione e l'utilizzo di tecnologie avanzate, analisi delle politiche relative alla loro acquisizione, report sui principali trend tecnologici (sia in UE che extra-UE), e acceso a centri tecnologici e hub di innovazione europei. Tali informazioni sono facilmente accessibili tramite l'ATI Website, spin off delle precedenti esperienze del KETs Observatory – una piattaforma che raccoglieva dati e informazioni sull'utilizzo di KETs dentro e fuori l'UE – e del Digital Transformation Monitor – un portale finalizzato all'analisi delle tendenze mondiali nella trasformazione digitale tramite la raccolta di statistiche, rapporti e iniziative sulle principali sfide e opportunità industriali, politiche tecnologiche nel settore[186]. L'ATI individua sedici tecnologie avanzate: tecnologie di produzione avanzata, Materiali avanzati, Intelligenza artificiale, Realtà virtuale e aumentata, Big Data, Blockchain, Cloud Computing, Connettività, Biotecnologia industriale, Internet of Things, Micro- e Nano-elettronica, Mobilità, Nanotecnologia, Fotonica, Robotica e Sicurezza. Per quanto concerne il settore tecnologico Sicurezza, si registra a livello europeo una maggiore frequenza nell'adozione di tecnologie avanzate rispetto agli altri settori (64.78% delle imprese europee e 61.29% delle industrie italiane)[187]. La capacità degli Stati membri di generare tecnologia innovativa in questo settore risulta invece minore rispetto alla media degli altri settori tecnologici (con il 21.87% delle patenti globali nel settore). Le innovazioni tecnologiche della sicurezza registrate nel database sono infatti avvenute prevalentemente nei settori economici della manifattura, dell'elettronica e dei macchinari, mentre la loro applicazione è più frequente nei settori delle telecomunicazioni, delle utilities e dei servizi finanziari[188].

Da ultimo, l'attenzione è concentrata sull'Osservatorio sulle Tecnologie Critiche che saranno in larga parte dual-use. Questo è inteso come di supporto all'Azione 4 del *Piano d'azione sulle sinergie* della CE, volta allo sviluppo di roadmap tecnologiche per l'innovazione a cavallo dei settori difesa, spazio e civile. L'osservatorio dovrebbe essere gestito dal Joint Research Centre (JRC) della CE, sede di Ispra in Italia, e dovrebbe raccogliere dati sulle tecnologie critiche emergenti in un rapporto classificato per gli Stati membri entro la fine del 2022 e con cadenza biennale. È importante definire i ruoli e le interazioni per usare al meglio lo strumento anche cercando di completare un profilo che

[186] CE, "Advanced Technologies for Industry"; Knowledge for policy (2018), "Key Enabling Technologies (KETs) Observatory", CE, 26 Gennaio; Confindustria Lombardia, "Portale europeo Digital Transformation Monitor"
[187] ATI, "Data Dashboard – Country Indicators"
[188] ATI, "Data Dashboard – Sectoral Indicators"

potrebbe risultare molto accademico in seno al JRC. Secondo alcuni esperti non è ancora chiaro come avverrà l'interlocuzione con l'industria che dovrebbe essere diretta. La scelta su quale tecnologia critica implementare deve partire dall'analisi delle capacità degli Stati membri, ma la scelta su quale tecnologia utilizzare per implementare determinate capacità dev'essere dell'industria. In altre parole, il rapporto classificato biennale sarà sostanzialmente un database relativo a capacità critiche da sviluppare a livello UE. Tuttavia, una volta stabilite, sarà necessario trasformare tali capacità in tecnologie e soluzioni. A tal fine è necessario il ruolo dell'industria che dovrà necessariamente avere visione del rapporto.

È importante considerare che ci sono diversi interessi da contemperare. Ad esempio, mentre il termine "critico" per alcuni riguarda aspetti di mercato, per altri concerne aspetti di strategia. È comunque già un notevole risultato mettere attorno a un tavolo diversi attori che dovranno rimodellare il fattore culturale per superare anni di strutture, approcci e regolamenti diversi, pur appartenendo almeno in parte allo stesso ecosistema. Secondo alcuni esperti, altro aspetto da considerare nella fase di attuazione è che il database rischia di fornire una fotografia, mentre le tecnologie critiche evolvono come un film: possono cambiare completamente, soprattutto in termini di value chain. Una volta stabilito che una tecnologia è necessaria per implementare una capability critica, si deve capire infatti come quella soluzione può essere implementata dal punto di vista dell'intera value chain quindi considerare, ad esempio, quali asset industriali e quali supply chain sono coinvolte, che tipo di controlli sono previsti, che tipi di relazioni e dipendenze strategiche tra Stati esistono – con priorità che cambiano e che influenzano i processi con cui si individua, implementa, migliora e modifica (in reazione a cambiamenti) una tecnologia critica.

GOVERNANCE FINANZIAMENTI PUBBLICI

I finanziamenti pubblici per R&S includono i settori civile/sicurezza, militare e dual-use. Una governance efficace ed efficiente è fondamentale per garantire coerenza, continuità e ottimizzazione delle risorse, e può orientare in modo incisivo R&S dual-use e/o trasferimento di tecnologie e prodotti dual-use. Ad oggi, però, a livello europeo continua a mancare un framework coerente[189]. È opportuno chiedersi su quali livelli si può immaginare un intervento pubblico volto a potenziare la performance della governance e quali possono essere gli obiettivi e le modalità di tale intervento.

[189] Fiott, D. e Ketselidis, M. (2022), "Eu Civil-Defence Synergies: Understanding the Challenges and Drivers of Change", ARES Group, IRIS, Marzo, p. 25

UE

Come realizzare al meglio la collaborazione tra CE e EDA in materia di finanziamenti per R&S continua ad essere oggetto di studio anche da parte delle Istituzione europee. Le riflessioni del Protection and Security Advisory Group (PASAG) si sono concentrate su alcuni aspetti di cui tener conto. La premessa è quella di riconoscere che sinergie dual-use sono possibili solo in alcune specifiche aree di comune interesse nel campo dei programmi di finanziamento sicurezza e difesa e decise caso per caso anche al fine di evitare inutili duplicazioni. Tali aree pur venendo generalmente riconosciute – come ad esempio cyber, CBRN, C4I/sorveglianza – dovrebbero essere ulteriormente chiarite e specificate dalla CE[190]. Si rilevano, infatti, problemi di definizione che ancora oggi, persistono al punto che non esisterebbe una comprensione comune della portata del dual-use e della sua trasposizione nei programmi europei di sicurezza e di difesa[191].

Alcune raccomandazioni pratiche sono di breve termine e riguardano il rafforzamento del coordinamento istituzionale già esistente tra servizi della CE responsabili dei programmi di sicurezza e quelli responsabili dei programmi di difesa, e tra CE ed EDA[192]. Altre, di lungo termine, puntano ad un coordinamento strategico preventivo sugli investimenti in aree dual-use tra i programmi sicurezza e difesa che sia basato su un meccanismo strutturato e istituzionalizzato che coinvolga comitati di programma e CE[193].

Il regolamento che istituisce Horizon Europe prevede disposizioni specifiche per le sinergie con altri programmi, illustrando nel suo Allegato IV alcuni meccanismi tra cui rilevano il Programma spaziale dell'Unione, l'ISF e l'Integrated Border Management Fund (IBMF). Le sinergie con l'EDF, a differenza di quanto indicato per gli altri programmi, sono volte ad evitare inutili duplicazioni[194]. Lo scopo delle sinergie dovrebbe riguardare i programmi dell'Unione sotto diversi aspetti, "dalla loro concezione e pianificazione strategica fino alla selezione, alla gestione, alla comunicazione, alla diffusione e allo sfruttamento dei risultati, alla sorveglianza, all'audit e alla governance del progetto. Per quanto riguarda il finanziamento delle attività di ricerca e innovazione (R&I), le sinergie dovrebbero consentire di armonizzare il più possibile le norme, anche in materia di ammissibilità dei costi. Allo scopo di evitare duplicazioni o sovrapposizioni, aumentare l'effetto leva del finanziamento dell'Unione e di ridurre gli oneri amministrativi per i richiedenti

[190] Pasag (2020), "Optimising access to dual-use R&T and R&D results for security", p.6
[191] Ivi, p. 10
[192] Ivi, p.7
[193] Ivi, p.8
[194] PE e Consiglio dell'UE (2021), "Regolamento (UE) 2021/695 che istituisce il programma quadro di ricerca e innovazione Orizzonte Europa e ne stabilisce le norme di partecipazione e diffusione, e che abroga i regolamenti (UE) n. 1290/2013 e (UE) n. 1291/2013", 28 Aprile

e i beneficiari, dovrebbe essere possibile promuovere sinergie, in particolare mediante finanziamenti alternativi, combinati, cumulativi e tramite il trasferimento di risorse"[195].

La CE, in una recente Comunicazione sul suo contributo alla difesa europea (2022), pone tra le misure e le azioni concrete da perseguire un maggiore sostegno alle sinergie tra dimensione civile e componente di difesa nella ricerca e innovazione e alla riduzione di dipendenze strategiche nelle tecnologie critiche[196]. In accordo con il *Piano d'azione sulle sinergie*, la CE ha annunciato che stabilirà un metodo per incoraggiare la dimensione del dual-use nella ricerca e innovazione a livello UE[197]. Il Piano stesso annuncia, entro il primo semestre 2022, l'avvio di un incubatore di innovazione dual-use per sinergie tra i tre settori civile, difesa e spazio e tra questi ed altri ecosistemi[198]. Ad esempio, esaminando i risultati di ricerca finanziata dall'UE e proponendo ulteriori finanziamenti per lo sviluppo, oppure promuovendone l'adozione presso utenti dei settori inversi con particolare attenzione all'innovazione dual-use proveniente da PMI, start-up e RTOs[199].

LIVELLO UE/LIVELLO NAZIONALE

Il Work Programme Security viene stabilito in maniera congiunta a partire da vari elementi tra cui input dalle piattaforme tecnologiche europee di riferimento, il Security Advisory Group (SAG), composto da personalità selezionate dalla CE sulla base dei curricula, i programmi di ricerca precedenti e le indicazioni dei cittadini che possono essere espresse via web. Successivamente, il Work Programme passa all'esame dei Comitati di Programma composti da esperti nei vari settori, nominati dagli Stati membri e incaricati dalla CE per garantire che gli Stati membri siano coinvolti e che sia data ampia diffusione e condivisione delle tematiche stesse a livello nazionale. Il Work Programme viene quindi approvato, dopo valutazione delle risorse e relativa compartimentazione budgetaria all'interno dei vari sotto-capitoli.

Una corretta governance sulle sinergie tra finanziamenti UE e nazionali sarebbe positiva. In tale contesto sarebbe significativo applicare il concetto di complementarietà – vale a dire ricercare una ottimale distribuzione delle competenze fra differenti stakeholder nazionali e comunitari al fine di massimizzare gli effetti dei finanziamenti ed evitare duplicazioni – e quello di supplementarietà – che permetta di mobilitare risorse aggiuntive

[195] PE e Consiglio dell'UE (2021), "Regolamento (UE) 2021/695 che istituisce il programma quadro di ricerca e innovazione Orizzonte Europa"
[196] CE (2022), "Contributo della Commissione alla difesa europea", 15 Febbraio, p.3 [punto che sarebbe dovuto essere discusso al vertice di Versailles 10-11 marzo 2022 dedicato poi invece all'ucraina]
[197] CE (2022), "Contributo della Commissione alla difesa europea", p.8
[198] CE (2021), "Piano d'azione sulle sinergie", p.14
[199] Ivi, p.13

rispetto ai finanziamenti stanziati. Ciò sembra rilevante al fine di evitare duplicazioni non volute, al contempo respingendo opinioni che ritengono che in presenza di finanziamenti europei quelli nazionali siano meno necessari. Secondo alcuni è, invece, importante prevedere anche eventuali sovrapposizioni di fondi per mantenere l'indipendenza nazionale per specifiche tecnologie, in particolare tecnologie sovrane, ovvero prodotti, processi e competenze che permettono a un Paese (ma anche ad un'istituzione sovranazionale, un'organizzazione o un'industria) di raggiungere un alto livello di autonomia e indipendenza da terzi. Sempre più frequentemente queste tecnologie vengono associate alle EDTs quali applicazioni di informatica, robotica e intelligenza artificiale. Alcuni ritengono, infatti, che questa limitazione delle duplicazioni debba essere attuata con misura, in modo da poter investire su più iniziative sullo stesso tema. Infatti, se da un lato meno duplicazioni possono significare più risorse da investire altrove, dall'altro un certo grado di ridondanza, con diversi attori coinvolti sullo stesso tipo di R&S, può portare a nuove prospettive. Secondo alcuni, addirittura una limitazione delle duplicazioni indiscriminata significherebbe limitare la libera e corretta concorrenza tra le aziende e privilegiare le lobby più potenti. Una possibilità potrebbe essere quella di non attuare semplici eliminazioni di duplicazioni dei finanziamenti, ma cercare di valorizzazione e sostenere in maniera trasparente elementi e progetti sinergici e dual-use.

ITALIA

La maggiore armonizzazione ed integrazione tra PNRM e PNR, indicata dal Libro Bianco per la sicurezza internazionale e la difesa nel 2015, non sembra aver avuto seguito[200]. Il MDIF ha comunque stretto accordi con il mondo accademico e avviato, con il MUR, un rapporto strutturato per attivare sinergie. Questo in un contesto in cui il SGD/DNA è "impegnato ad accrescere la coscienza dell'importanza della ricerca in ambito difesa ed a coinvolgere, nel perseguire l'obiettivo, tutte le risorse intellettuali, organizzative e finanziarie disponibili nel Paese, sfruttando le sinergie consentite da un approccio "trasversale" basato sulla possibilità di utilizzare per applicazioni diverse – civili, militari e dual-use – basi tecnologiche derivanti da una matrice di ricerca comune"[201]. Un simile approccio potrebbe anche in parte mitigare una situazione in cui lo stanziamento per la ricerca tecnologica militare risulta molto al di sotto dell'auspicabile livello indicato in ambito NATO ed europeo – 2% del budget Difesa – e si attesta, a livello nazionale, allo 0.2%.

[200] MDIF (2015), "Libro Bianco per la sicurezza internazionale e la difesa", Luglio
[201] MDIF, "la Ricerca & Innovazione"

Secondo alcuni, l'ipotizzata armonizzazione continuerebbe ad essere impossibile allo stato attuale delle cose, con PNR e PNRM completamente diversi nella concezione e nell'implementazione. Il PNRM è adottato annualmente, mentre il PNR ha di norma durata pluriennale. A PNR e PNRM corrisponderebbero inoltre database di conoscenze non sempre condivisibili. Alcuni ritengono che sarebbe più realistico un coordinamento tra le priorità dei due Piani, ma secondo altri al momento anche le priorità sembrano incompatibili e hanno proiezioni differenti nel tempo. Altri ancora osservano che l'armonizzazione è positiva nella misura in cui esalta elementi in comune e non forza convergenze non sostenibili tra ambito civile/sicurezza e militare. La giusta misura sarebbe dunque di non attuare semplici eliminazioni di duplicazioni dei finanziamenti, ma cercare di valorizzazione e sostenere elementi e progetti sinergici e dual-use.

Nonostante la mancanza di progressi in tal senso, la *Direttiva per la politica industriale della Difesa* riprende la questione del rapporto tra PNRM e PNR, stabilendo che il PNRM dovrà svilupparsi nel campo dell'aerospazio, difesa e sicurezza tenendo conto di possibili sinergie con il PNR, ma anche con i programmi di ricerca spaziale ASI e quelli di sviluppo tecnologico del MiSE, oltre che con le organizzazioni governative, accademiche e scientifiche nazionali[202]. A tal fine, la *Direttiva* richiede che le infrastrutture e le capacità di ricerca della Difesa vengano valorizzate e messe a disposizione per settori trainanti della tecnologia, anche civili, che potrebbero rivelarsi abilitanti pure ai fini militari[203]. Un maggiore raccordo tra MDIF e MUR (e CNR) sarebbe utile in entrambe le direzioni, a beneficio degli ambiti civile/sicurezza e militare. Infatti la Difesa, per TRL bassi, si avvale spesso dei laboratori del CNR, non avendo tuttavia visibilità su eventuali altre simili attività già finanziate in ambito PNR.

Il PNR 2021-2027 risulta semplificato rispetto al Piano precedente, passando da una tassonomia della ricerca applicata composta da 12 aree ad una che, ricalcando la struttura di Horizon Europe, si concentra su 6 cluster[204]: salute; cultura umanistica, creatività, trasformazioni sociali, società dell'inclusione; sicurezza per i sistemi sociali; digitale, industria, aerospazio; clima, energia, mobilità sostenibile; prodotti alimentari, bioeconomia, risorse naturali, agricoltura, ambiente.

Anche in ambito spaziale esiste un certo livello di incertezza riguardante il legame diretto tra PNR e investimenti nel settore, ed una frammentazione tra ASI, fondi al CIRA tramite PRORA, fondi MiSE, attività del CNR e fondi trasferiti ad ESA. Ancora in ambito

[202] MDIF (2021), "Direttiva per la politica industriale della Difesa", p.11
[203] Ibid.
[204] MUR, "Programma Nazionale per la Ricerca 2021-2027"

spazio, il PNR 2021-2027 ha seguito le indicazioni governative e ripreso le aree strategiche di interesse nazionale nelle quali investire. Per quanto riguarda il PNRM, pur mancando indicazioni e fonti certe, c'è l'impegno della Difesa italiana nel seguire alcune delle priorità nazionali in modo da stimolare ulteriormente la ricerca in campo spaziale, con potenziali ricadute anche in campo dual-use[205].

Secondo alcuni, un importante strumento che potrebbe consentire di ottimizzare i finanziamenti pubblici sarebbe il pre-commercial procurement che permette iniziative di ricerca applicata finalizzate ad una vera e propria industrializzazione con successiva acquisizione da parte dell'appaltante pubblico della soluzione progettata, unendo quindi in un unico percorso ricerca, sviluppo e industrializzazione, e il procurement vero e proprio. In questo modo si migliorerebbe il ritorno sull'investimento fatto. Resta inoltre sempre auspicabile attrarre anche investimenti privati pur considerando che la governance dei finanziamenti pubblici in R&S non può essere collocata al di fuori di chi gestisce le esigenze: tecnologie e prodotti devono essere una risposta ad esigenze concrete e nella stessa direzione può essere letta la crescente (e obbligatoria) presenza di end-user nei consorzi dei progetti finanziati da Horizon Europe. Alcuni ritengono che per quanto riguarda la R&S, nell'ambito della ricerca abbiano maggiore rilevanza gli attori pubblici, mentre nello sviluppo gli attori privati e il mondo industriale, con interessi contrastanti e in un contesto di rischi e di mancanza di comunicazione tra Difesa e MiSE con conseguente possibilità di duplicazione dei finanziamenti.

VISIBILITÀ E SEMPLIFICAZIONE

Lato pubblico, sarebbe positivo assicurare un'adeguata visibilità delle opportunità pubbliche di finanziamento per R&S e procurement (dual-use, ma anche del mercato inverso, sia a livello europeo che italiano), una semplificazione delle regole di ammissibilità (per facilitare l'accesso da parte di nuovi soggetti, anche del mercato inverso) e supporto tecnico (gratuito o a costi contenuti) alle imprese, in particolare alle PMI. Secondo alcuni, questo sarebbe un problema particolarmente sentito a livello italiano per la scarsa visibilità delle informazioni e la mancanza di interlocutori lato pubblico. In tal senso anche sul PNRM il processo di approvazione risulta complesso e articolato e di difficile gestione per realtà come start-up e PMI. Negli ultimi due anni sono state poste in essere azioni concrete (punteggio premiale per PMI nel 2021 e per PMI e Startup nel 2022) per incentivare la

[205] Si veda: La Rocca, G. e Marrone, A. (2022), "Italy and space, a strong position to enhance", in Marrone, A. e Nones, M. (ed.), "The Expanding Nexus between Space and Defence", IAI, Febbraio

partecipazione di tali realtà. Si tratta di una strada intrapresa molto positiva, cui si potrebbero unire iniziative del tipo consulenze, corsi, facilitatori.

A livello europeo, la necessità di incrementare la visibilità ed interpretazione delle opportunità di R&S dual-use è chiara da alcuni anni. Sul fronte EDA è possibile ricordare, ad esempio, una Invitation to Tender del 2013 volta a contribuire ad una migliore comprensione degli aspetti dual-use della supply chain della EDTIB "better understanding of dual-use aspects of the European Defence Technological and Industrial Base (EDTIB) supply chain"[206]. L'HLG-KET Working Group on accelerating dual-use potential of KETs ha prodotto raccomandazioni e input per la CE su applicazioni dual-use delle KETs[207]. Queste includevano la richiesta alla UE e agli Stati membri di incrementare la visibilità delle opportunità di R&S dual-use nei bandi di ricerca, stabilire un inventario di quelle parti di Work Programmes con potenziale dual-use e predisporre analisi ex post che individuassero progetti finanziati da fondi europei con potenziale dual-use che potessero essere ulteriormente utilizzati e commercializzati. Come fondi europei si considerava H2020 e quindi ora applicabile anche ad Horizon Europe, oltre gli ESIFs. Secondo molti, tanto la visibilità dual-use nei bandi quanto l'analisi e le stime ex post sono obiettivi complessi da raggiungere. La questione delle analisi ex post è rilevante ed attuale, anche oltre il focus specifico sul dual-use. Recentemente (dicembre 2021) la CE ha individuato alcune misure volte al rafforzamento della sicurezza attraverso la ricerca e l'innovazione. Tra queste rientra l'impegno di incrementare la visibilità e tracciabilità dei risultati della ricerca coinvolgendo meccanismi europei e autorità nazionali per rendere più agevole una misurazione dell'impatto positivo degli investimenti europei[208].

La questione della visibilità delle opportunità di finanziamento rientra tra quelle affrontate anche dal *Piano d'azione sulle sinergie* della CE sulle sinergie tra l'industria civile, della difesa e dello spazio in particolare per facilitare PMI, start-up e RTOs in programmi UE nel settore spazio, difesa e industria civile connessa[209]. Tale supporto prevede iniziative (Azione 3) che vanno dagli strumenti interattivi multilingue per finanziamenti UE alla creazione di punti focali nazionali per la partecipazione ad EDF, oltre supporto tecnico e formazione pratica per le PMI, start-up e RTOs interessate alla partecipazione a tali programmi[210].

---

[206] Europe Economics (2014), "Enhancing support to SMEs",
[207] CE (2015), "High Level Expert Group on KETs publishes final recommendations", 24 Giugno
[208] CE (2021), "Enhancing security through research and innovation", 15 Dicembre, p.19
[209] CE (2021), "Piano d'azione sulle sinergie", p. 7
[210] Ivi, p. 8

Il tema della semplificazione dovrebbe considerare anche l'approccio allo screening dual-use nelle proposte di ricerca. In tale contesto infatti, secondo alcuni, la separazione culturale tra sicurezza e difesa è quasi tutta delle istituzioni e in minima parte dell'industria (quando si parla di aziende che trattano sicurezza e difesa e a maggior ragione se trattano spazio). In un certo senso, avere ricerca in sicurezza e ricerca in difesa separate sembra essere l'antitesi del dual-use. Le regole dovrebbero tener conto che, nell'ambito della ricerca, è difficile poter pensare e dichiarare che tutto non sia dual-use a livelli bassi di TRL. Regole che stabiliscono, ad esempio, che la EIB può finanziare attività dual-use solo se si dimostra che la loro applicabilità è maggiore nell'ambito civile rispetto a quello della difesa, possono sembrare vincoli e regolamenti di pre-concetto culturale. Spesso, infatti, non è possibile fare simili valutazioni a bassi livelli di TRL. Regole di questo tipo pongono parametri difficili da gestire e che minacciano la competitività dell'industria, nei confronti di Paesi extra-UE che abbiano un approccio diverso.

NORMATIVE

Alcune raccomandazioni sono focalizzate sulla possibilità di azioni lato pubblico – incluse posizioni italiane in UE – che possano influenzare positivamente anche conoscenza e compliance aziendale. Considerando la prospettiva delle organizzazioni pubbliche alcuni sottolineano infatti che, se è vero che la conoscenza da parte dell'azienda è la base della compliance, l'aspetto decisivo è – per tutti i tipi di policies e normative – la semplificazione e l'armonizzazione di norme e processi al fine di aumentare la consapevolezza degli operatori economici, non assorbire inutilmente risorse aziendali e non ritardare l'ingresso sul mercato e il soddisfacimento degli impegni presi. Questo deve essere tenuto sempre presente anche nella trasposizione ai livelli nazionali di normative UE. Da ultimo, nel 2022 la CE ha esortato gli Stati membri a convergere verso pratiche di controllo delle esportazioni simili e semplificate, segno che ancora sono necessari sforzi in tale direzione[211].

NORMATIVE EXPORT DUAL-USE

Il regime, nato negli anni '90, si basava originariamente su preoccupazioni di uso improprio del potenziale dual-use, ovvero sulla valutazione del rischio che un bene dual-use potesse essere impiegato a contributo della proliferazione di armi di distruzione di massa, ed è stato dunque impostato in maniera primaria in un'ottica di controllo. Successivamente si è fatta strada tra gli stakeholder l'opportunità di favorire la responsabile esportazione dual-

[211] CE (2022), "Contributo della Commissione alla difesa europea", p.4

use per la competitività del settore industriale europeo al punto che, secondo alcuni, il dual-use non può essere considerato un driver economico europeo se il regime di export control continuerà ad avere l'impostazione di controllo mantenuta finora, senza porsi anche come un facilitatore del trasferimento tecnologico – un'impostazione che richiederebbe l'accordo del Directorate General for Trade (DG TRADE) della CE, oltre ovviamente al supporto politico. Il nuovo Regolamento, entrato in vigore nel settembre 2021, è ancora troppo recente per poter valutare su medio periodo il reale impatto su questo ultimo aspetto. Con tale premessa, sul punto si raccolgono pareri in parte contrastanti. Alcuni ritengono che il Regolamento faciliti ulteriormente le esportazioni semplificando l'ottenimento delle licenze – in particolare grazie all'aumento del numero di possibili AGEU, con l'introduzione di una tipologia di autorizzazione globale per la realizzazione "Grandi Progetti", sebbene ancora poche aziende se ne stiano servendo – e soprattutto, tramite una maggiore condivisione delle informazioni tra Stati e l'intensa attività di outreach nei confronti delle PMI e di Paesi partner, promuovendo una parità di condizioni fra imprese esportatrici. Altri considerano che, almeno dalla sua impostazione teorica, il Regolamento sembri contenere elementi volti invece a rafforzare l'ottica di controllo. In tale direzione sarebbero da intendere, ad esempio, il notevole aumento delle pagine dell'Allegato I relativo agli item sottoposti a controllo, ma anche l'applicazione della clausola catch-all ad un ulteriore settore, quello della sorveglianza informatica. Tale estensione seguirebbe altre, già effettuate negli anni passati, con un approccio che va oltre l'originario scopo primario di controllo della clausola volto ai soli casi di violazione dei diritti umani. Secondo altri, la clausola catch-all rappresenterebbe comunque un esempio di successo per l'engagement del settore privato, di come l'esportatore possa sviluppare consapevolezza e responsabilità decidendo di segnalarne la possibile applicazione all'autorità competente.

Un altro aspetto, che potrà essere valutato solo a livelli di operatività maggiori del nuovo Regolamento, è il rischio di difformità di applicazione della normativa e delle liste. Ai livelli nazionali, questa può dipendere da due fattori collegati. Da un lato, le diverse trasposizioni del regime o meglio, trattandosi di un regolamento e dunque direttamente applicabile, le diverse pratiche amministrative di applicazione che quindi implicano differenti procedure di valutazione delle richieste di licenza di esportazione e del loro rilascio. Questo può comportare che uno Stato membro consideri dual-use quello che un altro considera invece militare, per motivi politici o di sovranità tecnologica. Ad esempio in Germania, a differenza dell'Italia, si considerano dual-use anche componenti non dual-use di prodotti complessi dual-use. Questo è basato anche su diversi approcci culturali con un risultato che, secondo alcuni, influenza la possibilità di trasferimento tecnologico.

Dall'altro lato, le procedure si basano su interpretazioni di concetti e termini chiave sia della normativa che degli item delle liste non sempre sufficientemente armonizzati ai livelli nazionali. Il risultato è un'applicazione della normativa complicata da duplicazioni provenienti sia dal fattore clausola catch-all applicata da ogni Stato membro secondo la propria indipendente valutazione, che dalla presenza di liste nazionali, oltre a quella UE, stabilite in alcuni Stati membri. L'Italia non ha mai considerato finora la possibilità di adottare una lista aggiuntiva nazionale ed il fatto di non aggiungere nulla di diverso a quanto previsto dall'UE evidenzia una posizione equilibrata e favorevole all'uniformità. A proposito della clausola catch-all, ad esempio, in ambito sorveglianza informatica, è il Regolamento stesso a porre la questione di una maggiore armonizzazione dell'applicazione a tal fine raccomandando agli Stati membri di scambiare informazioni tra loro e con la CE.

Quanto sopra può generare incertezza sulle applicazioni delle disposizioni, con rischio di effetti distorsivi sulla concorrenza delle imprese operanti nel settore. Si pensi al caso di imprese europee operanti in regimi nazionali più stringenti o complessi, sia dal punto di vista della trasposizione delle normative che dell'applicazione delle stesse (ad esempio durata dei controlli), che dunque risultano penalizzanti soprattutto sull'abilità delle imprese di competere internazionalmente. Quanto a competitività, bisogna anche ricordare che, anche se il regime riguarda in primis il sistema di export verso Paesi extra-UE, esso include anche una lista per trasferimenti intra-UE. Anche in questo caso, stakeholder del settore da tempo esprimono la necessità di modalità di controllo che non ostacolino la libera circolazione di tecnologie e prodotti nel mercato unico europeo[212]. In tale contesto, il peso di un'armonizzazione avrebbe un effetto amplificato, in quanto i partner extra-europei percepirebbero l'industria europea come un unico attore – almeno da un punto di vista dell'export control – attribuendogli un maggior grado di affidabilità a prescindere dallo Stato membro con il quale si interfacciano. Tale ragionamento è rafforzato dal fatto che l'Europa si rapporta con partner extra-europei specialmente attraverso consorzi/programmi intergovernativi i quali, solitamente, se da una parte prevedono un capofila, dall'altra rappresentano la somma di più industrie nazionali soggette a proprie applicazioni nazionali potenzialmente diverse anche se sono trasposizione dello stesso regolamento UE.

Le difficoltà di stabilire definizioni condivise può inoltre impattare sull'ottimale ed uniforme attuazione dei regimi di controllo e di embargo e quindi sulla sicurezza internazionale cui il nuovo Regolamento sembra attribuire rinnovata importanza. La definizione di "esportatore" ora include anche qualsiasi persona fisica che trasporti prodotti

[212] ASD (2014), "The review of the dual-use export control policy of the European Union", 22 Ottobre

o tecnologie dual-use nel proprio bagaglio personale[213]. Per favorire la corretta applicazione, il Regolamento rende obbligatori gli Internal Compliance Programmes (ICPs) in caso di autorizzazioni globali e della AGEU 007 che riguardano l'esportazione intragruppo societario di software e tecnologia. È infatti da considerare che mentre per l'export degli armamenti c'è una autorizzazione alle trattative, nell'export dual-use l'autorizzazione è appunto all'esportazione e riguarda quindi un passaggio solitamente collocato a contratto già firmato.

Considerati i rischi descritti su controlli e concorrenza in ambito export dual-use, è importante che, lato pubblico, si intraprendano azioni per la semplificazione e l'armonizzazione delle prassi amministrative nazionali di applicazione del Regolamento e la definizione di interpretazioni condivise. Resta necessaria, infatti, la definizione di concetti comuni fra istituzioni europee e nazionali per assicurare la corretta implementazione della normativa[214]. Secondo alcuni, armonizzazione e interpretazioni condivise potrebbero essere supportate da piattaforme e tool informatizzati coordinati ed allineati tra i diversi Stati membri per aumentare l'efficienza dei processi, ma pima ancora ci deve essere una volontà politica, che non appare scontata. Le iniziative di centralizzazione presso la CE, infatti, non sono sempre state sostenute dagli Stati membri. La materia export dual-use è generalmente ritenuta una prerogativa nazionale come la materia export armamenti.

Il settore pubblico potrebbe finanziare anche iniziative di sensibilizzazione e la messa a disposizione (gratuita) di consulenze, corsi, facilitatori, helpdesk organizzati dalle autorità di controllo. Secondo alcuni, la formazione è centrale. Altri ritengono che il tema debba essere impostato in maniera più ampia e considerano che in Italia sarebbe utile una Scuola di formazione a livello universitario sul trade compliance in senso lato, per la formazione di esperti su una knowledge comune. Si segnala inoltre l'opportunità, secondo altri, di dotare di una formazione in parte comune i funzionari che lavorano nei due diversi settori delle autorizzazioni e delle dogane. Questo soprattutto a beneficio di PMI generalmente dotate di minori mezzi per accedere a consulenti e studi rispetto alle grandi aziende che più facilmente possono facilitare la compliance mediante l'assunzione di un compliance officer esterno o formandone uno interno o tramite l'acquisizione di programmi gestionali dedicati. Senza considerare i grandi gruppi industriali dotati di trade compliance office strutturati e dedicati. Al fine di assistere le imprese in questo processo, il CNR offre pareri tecnici, non

[213] Si veda: PE e Consiglio dell'UE (2021), "Regolamento (UE) 2021/821 che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso (rifusione)"

[214] Bromley, M. e Brokmann, K. (2021), "Implementing the 2021 recast of the eu dual-use regulation: challenges and opportunities", SIPRI, Settembre

vincolanti, mirati a chiarire dubbi sul carattere dual-use di un determinato prodotto, dunque sulla necessità di richiedere una licenza per l'esportazione[215]. In tale contesto è da segnalare come molto positiva l'iniziativa del Ministero degli affari esteri e della cooperazione internazionale (MAECI) che a breve lancerà l'"e-licensing", ovvero il nuovo portale per la gestione completamente informatica delle autorizzazioni all'esportazione di beni e tecnologie a duplice uso.

La materia continua, però, ad essere troppo poco conosciuta. C'è poca consapevolezza, soprattutto nelle PMI che spesso sono quelle che hanno tecnologie e conoscenze dual-use. Si tratta invece di una normativa rilevante. In tema dual-use, infatti, il Decreto-Legge 21 marzo 2022, n. 21, *Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina*[216] ha stanziato fondi per il potenziamento del personale di formazione ingegneristica presso il MAECI e disciplinato il potere di ispezione presso le aziende. L'amministrazione dei fondi relativi alle nuove risorse rappresenta sicuramente un aspetto positivo, ma di grande responsabilità nella gestione. I profili tecnici richiesti, che dovranno essere formati sulla normativa, potrebbero coprire aree di competenze quali il nucleare, le armi chimiche, l'informatica (cyber) e l'ambito missilistico.

A livello italiano, dal 1° gennaio 2020, l'autorità preposta alla valutazione e rilascio di licenze per l'esportazione di prodotti e tecnologie dual-use è passata dal MiSE all'Unità per le autorizzazioni dei materiali di armamento (UAMA) del MAECI[217]. Tutto il personale dedicato in ambito MiSE è transitato al MAECI così mantenendo intatta la competenza con una forte identità della Divisione. Il passaggio risponde ad una riconosciuta esigenza di garantire maggiore sintonia tra la politica estera e la politica esportativa di tutti i beni sensibili (armamenti e prodotti dual-use)[218] con una nuova attenzione sulle questioni di sicurezza e del diritto internazionale. In effetti, come nel caso più recente delle sanzioni alla Russia, i beni dual-use sono stati tra i primi ad essere interessati dalle nuove misure, con l'estensione del divieto di esportazione di beni duali dagli enti militari agli enti civili. Il passaggio, più in generale, sembra in linea con i compiti, già in capo al MAECI, di sostegno alle imprese per l'internazionalizzazione. Secondo alcuni, l'accorpamento in UAMA anche del controllo

---

[215] Consulsped (2010), "Restrizioni alle esportazioni e alle importazioni v/Iran", 14 Luglio; Studio Legale Tomasi, "Dual Use – Prodotti a Duplice Uso"

[216] Gazzetta Ufficiale (2022), "Decreto-Legge 21 Marzo 2022, n.21, Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina", 21 Marzo

[217] Gazzetta Ufficiale (2019), "Decreto-Legge 21 Settembre 2019, n.104, Disposizioni urgenti per il trasferimento di funzioni e per la riorganizzazione dei Ministeri per i beni e le attivita' culturali, delle politiche agricole alimentari, forestali e del turismo, dello sviluppo economico, degli affari esteri e della cooperazione internazionale, delle infrastrutture e dei trasporti e dell'ambiente e della tutela del territorio e del mare, nonche' per la rimodulazione degli stanziamenti per la revisione dei ruoli e delle carriere e per i compensi per lavoro straordinario delle Forze di polizia e delle Forze armate e per la continuita' delle funzioni dell'Autorita' per le garanzie nelle comunicazioni.", 21 Settembre

[218] Studio Legale Padovan (2019), "Trasferimento di competenze dal MiSE al MAECI: pubblicazione della l. 132/2019 – le novità per il dual-use", 29 Novembre

sull'export dual-use comporta il vantaggio di poter assicurare un approccio olistico con l'export di beni militari, specialmente nei casi in cui sia labile il confine fra natura duale o strettamente militare di determinati beni.

Allo stesso tempo, questa impostazione potrebbe, secondo alcuni, comportare il rischio, da un lato, di portare ad un contenimento delle esportazioni dual-use e, dall'altro, di innescare inefficienti contaminazioni tra il regime di controllo delle esportazioni militari (da sempre gestito da UAMA) e quelle dual-use. Il cambiamento potrebbe quindi essere letto come un aumento del livello di controllo. Più in generale, la scelta del passaggio da MiSE a MAECI sembra rispecchiare un'impostazione da Paese importatore, diversa rispetto a Paesi ad alta vocazione esportativa in cui tale funzione è collocata presso Ministeri che si occupano di commercio e industria.

Il MiSE è in via di riorganizzazione nel momento in cui si scrive. Nel nuovo assetto, il fatto di non avere più tra i propri compiti quello sulle licenze per export dual-use non dovrebbe intaccare l'attenzione del Ministero per questo settore. Nel quadro della politica industriale e del sostegno all'innovazione tecnologica nazionale, il MiSE potrebbe utilmente e con competenza assicurarvi tutta l'attenzione che merita. In tale contesto, come confermato da più parti, sarebbe utile un'attenzione specifica alle PMI, con meccanismi procedurali, amministrativi e finanziari dedicati.

NORMATIVE IPRs

Come visto, la definizione di diritti di proprietà intellettuale impatta fortemente sulla possibilità di realizzare trasferimenti di tecnologia anche da dal settore civile/sicurezza a militare e viceversa, soprattutto nell'ambito di progetti UE o multinazionali. La maggioranza dei rappresentanti industriali, ma anche della Difesa, sono nettamente concordi nel considerare gli IPRs come una priorità.

Gli IPRs nel in campo militare sono trattati in maniera diversa dal settore civile/sicurezza. Le difficoltà che ne derivano, in termini di passaggio da un settore all'altro, possono essere un disincentivo per gli stakeholder perché non sono esclusi casi di ritardi, anche di anni, poco sostenibili da parte di PMI in particolare, che possono anche rinunciare completamente ad intraprendere un progetto. Secondo alcuni, il problema dei differenti regimi IPRs, tra mondo militare e civile/sicurezza, potrebbe essere facilitato dall'esistenza degli standard ibridi.

In ambito di finanziamenti pubblici si deve puntare ad una definizione degli IPRs quanto più possibile chiara, univoca, accessibile, armonizzata a livello UE per facilitare aperture a collaborazioni sia intra-UE che rispetto ad interlocutori extra-UE. In particolare, le PMI

dovrebbero essere supportate nella comprensione, definizione e gestione degli IPRs. Secondo alcuni, un possibile modello positivo a livello UE potrebbe essere ispirato a quello degli IPRs SME Helpdesks finanziati dal bilancio UE dedicato al programma Competitiveness of Enterprises and Small and Medium-sized Enterprises (COSME), per fornire consulenza e formazione sugli IPRs a ricercatori e PMI europee che partecipano a bandi europei o coinvolte in processi di trasferimento tecnologico a livello internazionale[219]. A livello nazionale, alcuni ritengono che la stessa necessità potrebbe prevedere un potenziamento del ruolo del MiSE.

DEFINIZIONI

Quello delle definizioni e terminologie comuni si conferma un aspetto di fondamentale importanza anche per R&S dual-use e/ trasferimento di tecnologie e prodotti dual-use. Definizioni e terminologie comuni – almeno all'interno della stessa categoria di stakeholder e per le stesse finalità (es. monitoraggio tecnologico) – aiutano la definizione di parametri per l'ottenimento di quadri coerenti e misurabili. Non sono facilmente ottenibili e devono comunque essere considerate come dinamiche. Le implicazioni riportate sono diverse e investono tutti i maggiori fattori che possono influire su R&S dual-use e/o trasferimento di tecnologia e prodotti dual-use. Porre l'attenzione sulle molteplici definizioni di dual-use e sulla mancanza di definizioni comuni, è rilevante perché queste possono impattare negativamente sulla governance e/o su importanti aspetti organizzativi e gestionali. Di volta in volta si possono rilevare temi prioritari collegati alla questione delle definizioni e terminologie comuni e resta aperta e attuale la questione di come strutturare interventi pubblici volti all'ottenimento di definizioni e terminologie comuni. Tra i fattori coinvolti vi sono, tra gli altri, l'efficacia della domanda, del monitoraggio tecnologico, della governance dei finanziamenti pubblici, delle normative. Quanto alla domanda, definizioni e terminologie comuni sono ritenute di fondamentale importanza per la comprensione di esigenze, funzioni, requisiti e dei livelli di maturità tecnologica dei due ambiti civile/sicurezza e militare. Quanto al monitoraggio tecnologico favoriscono, o a volte sono condizione per, la validità di strumenti di politica tecnologica ed industriale.

Quanto alla governance dei finanziamenti pubblici e in particolare l'accesso a finanziamenti di R&S, la *Guidance note - Research with an exclusive focus on civil applications* sulla eligibilità di ricerche nel quadro di H2020 riportava "If your research is intended to be used in military application or aims to serve military purposes, it cannot be

[219] Si veda: CE, "COSME- Europe's programme for small and medium-sized enterprises"

funded under Horizon 2020. As long as your research is intended for non-military activities, it could be eligible for funding. Projects involving the defence industry or military organisations are not automatically excluded from funding. Research on defence related subjects may still qualify for funding, as long as its aims are exclusively focused on civil applications"[220]. Queste indicazioni non sono così dirimenti e ci si potrebbe chiedere cosa siano le military e non-military activities, visto che in alcuni contesti compiti di sicurezza interna ed esterna non hanno confini netti e che probabilmente i compiti istituzionalmente assegnati alle FFAA possono differire da Stato a Stato. Vanno tenuti presenti diversi fattori che confermano come la mancanza di riferimenti condivisi possa avere impatti negativi anche sull'orientamento degli stakeholder pubblici e privati nei bandi di ricerca: tra gli altri, la mancanza di dati ufficiali sui finanziamenti UE per le tecnologie dual-use; l'attenzione posta dall'EDA a chiarire "dual-use aspects of the European Defence Technological and Industrial Base (EDTIB) supply chain"[221]; la raccomandazione dell'HLG-KET Working Group on accelerating dual-use potential of KETs di aumentare la visibilità delle opportunità di dual-use e di predisporre analisi ex-post che individuino progetti finanziati da H2020 e/o dagli ESIFs con potenziale dual-use che possano essere ulteriormente utilizzati e commercializzati; la pubblicazione delle due guide da parte di EDA e CE nel 2014, e le altre due guide CE del 2017, per l'utilizzo di fondi UE a scopo dual-use.

Quanto alle normative, la mancanza di definizioni comuni può implicare effetti distorsivi su efficacia ed efficienza del controllo delle esportazioni e sull'applicazione uniforme degli embarghi, oltre che sulla concorrenza. L'uso dei termini civile/sicurezza, militare, dual-use è determinato in base a definizioni giuridico-burocratiche quali ad esempio i regolamenti sul controllo dell'export militare: tecnologie e prodotti militari sono inclusi nelle liste di tecnologie militari e per trasformare un item da militare in civile/sicurezza, questo deve essere declassato alla lista "civile" esportabile. La questione delle definizioni e terminologie comuni è ampia e, come visto nel caso delle tecnologie dual-use, oltre riguardare cosa si intenda per "dual-use", può riguardare anche il solo termine "tecnologia". Non solo, problemi di definizioni esistono anche a livello di documenti ufficiali e possono includere una non chiara distinzione dei differenti piani delle "tecnologie" e delle "applicazioni". Anche l'uso di tassonomie ha reso evidente che, pur quando condivise (per esempio in ambito EDA si pone molta attenzione alla tassonomia relativa alla ricerca tecnologica), queste non sono poi sempre interpretate in maniera univoca: i significati possono variare in base all'ambito e alle finalità delle analisi e restano soggetti a diverse interpretazioni che evolvono nel tempo.

---

[220] CE (2015), "Guidance note — Research with an exclusive focus on civil applications", Novembre

[221] Briani, V., Marrone, A., Moelling, C. e Valasek, T. (2013), "The development of a European Defence Technological and Industrial Base (EDTIB)", PE

Nota sull'IRAD e Nota sulle Autrici

IRAD[222]

L'Istituto di Ricerca e Analisi della Difesa (IRAD) è l'Organismo che gestisce, nell'ambito e per conto del Ministero della Difesa, la ricerca su temi di carattere strategico.

Costituito come Centro Militare di Studi Strategici (Ce.Mi.S.S.) nel 1987 e riconfigurato come IRAD nel 2021 a seguito dell'entrata in vigore della Legge 77/2020 - art. 238 bis, l'IRAD svolge la propria opera avvalendosi di esperti civili e militari, italiani ed esteri, in piena libertà di espressione di pensiero.

Quanto contenuto negli studi pubblicati riflette quindi esclusivamente l'opinione del Ricercatore e non quella del Ministero della Difesa.

Federica Di Camillo

Federica Di Camillo è Vicedirettore dell'Istituto Affari Internazionali, Responsabile del Programma "Sicurezza" e Responsabile di ricerca nel Programma "Difesa". Si occupa di sicurezza e difesa a livello nazionale ed europeo con particolare riguardo ad istituzioni e policies, R&S&I e mercati della sicurezza, tecnologie duali e minacce non convenzionali (CBRN). Selezionata dal Dipartimento di Stato statunitense per l'International Visitor Leadership Program su "U.S.-European Security Issues" (2010). Giurista di formazione in Italia, ha svolto periodi di studio presso l'Università Panthéon-Assas (Parigi) e ha conseguito un Dottorato di ricerca in Ingegneria della Produzione Industriale, presso la Facoltà di Ingegneria dell'Informazione, Informatica e Statistica dell'Università degli Studi di Roma "La Sapienza", con una Tesi su "L'influenza dei fattori organizzativi e gestionali nei processi di innovazione dual-use".

Ottavia Credi

Ottavia Credi è Ricercatrice Junior nei Programmi "Sicurezza" e "Difesa" dell'Istituto Affari Internazionali. Si occupa prevalentemente di sicurezza internazionale, difesa transatlantica ed europea, anti-terrorismo, minacce CBRN e non-proliferazione. Ha svolto tirocini presso il DG EXPO del Parlamento europeo a Bruxelles e l'American Security Project a Washington DC. Ha conseguito una laurea in Studi Internazionali presso l'Università degli Studi di Trento e un Masters of Arts in Intelligence & International Security presso il War Studies Department del King's College London.

[222] MDIF, "Istituto di Ricerca e Analisi della Difesa"

ISBN 979-12-551-5004-6